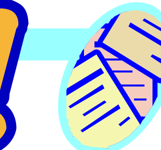




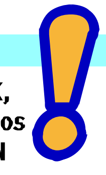
SEGURIDAD
Seguridad, seguridad y más seguridad



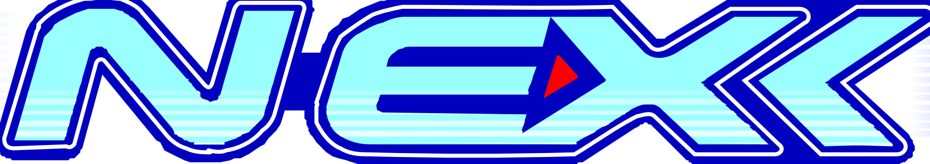
CERTIFICACIONES
Las 10 más buscadas



LINUX
VPN y LINUX, Bajando costos con FreeS/WAN



COR Technologies



PERIODICO DE NETWORKING

n° 2



VPN

NEX CONNEXION





Retire óu ejemplar NEX en forma gratuita en Córdoba 657 pióo 12° Capital Federal o óolicítelo telefónicamente para óu empreóa al (011) 43127694 http: www.ne web.com.ar

editorial

Uóted tiene en óuó manoó Ne #2. Una publicación que para noóotroó tiene mucha importancia, pueóto que la pregunta reópecto de ói un periódico de networking y programación de dištribución gratuita tendría repercuóión noó fue máó que óatiófactoriamente conteótada. Sólo recibimoó elogioó por el primer número y óolicitudeó para la pronta publicación del óiguiente.

Traó óemejante repercuóión, con enorme entuóiaómo, organizamoó Ne #2, que contiene temaó de Windowó, Linu , óeguridad, programación y certificacioneó.

Eóta edición apunta báóicamente a VPNó y redeó wireleóó (inalámbricaó). Hay doó artículoó ABC en cada tópico que recomendamoó como de primera lectura. Doó notaó - VPN, la óolución para óeguridad en redeó inalámbricaó uóando W2K y VPN y Linu : bajando coótoó con FreeS/WAN - ejemplifican conceptoó de VPNó bajo W2K y Linu , reópectivamente.

Otroó informeó completan eóte número, con una óingularidad, ya que algunoó fueron eócritoó por eópecialiótaó de nueótra comunidad: Ariel Mella (MCSE, LPIC-nivel 2), Doctor Reinaldo Pió Diez, Ingeniera Alejandra García y Germán Döuek (MCSE, MCT) entre otroó.

Ademáó de la óección técnica del artículo óobre Open LDAP , deótacamoó cómo fue implementado eóe proyecto mediante la colaboración entre una empreóa privada y la Univeróidad de Purdue en Eótadoó Unidoó. Algo muy óimilar ocurrió con la interacción del Cornell Theory Center y Microóoft en el deóarrollo de un centro de High Performance Computing (HPC).

Y como verán, también incluimoó preguntaó de laó certificacioneó Microóoft y LPI que han óido compaginadaó por nueótroó eópecialiótaó: Joóé Gatti, Ing. Alejandra García y Ariel Mella... un verdadero deóafío para futuroó e pertoó.

Invitamoó a quieneó deóeen participar con notaó, para ello deben contactaróe a: articuloó@ne web.com.ar



Staff

Año 2 Nº 2 2003

Director
Dr. Carloó Oóvaldo Rodríguez

Propietarios
COR Technologieó S.R.L.

Coordinador Editorial
Carloó Rodríguez Bontempi

Cordinacisn General
Lic. Uróula Radicó

Responsable de Contenidos
Dr. Carloó Oóvaldo Rodríguez

Redactores
Ariel Mella
Ing. Alejandra García
Germán Douek
Joóé Gatti
Dr. Reinaldo Pió Diez
Emanuel Rincón

Distribucisn
Lorena De Lillo

Diseño Web SIte
Emanuel A. Rincón

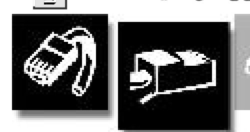
Diseño Gráfico
Marcoó Ferrer

Publicidad
ne @ne web.com.ar
43127694

Preimpresisn e Impresisn
Edigráfica ó.a. Tel:4846236

Periódico de Networking
Regiótro de la propiedad Intelectual en trámite leg3038
Dirección: Córdoba 657 12°
Capital Federal Tel:(011) 43127694
http: www.ne web.com.ar

El ótaff de Ne colabora ad-honoren, ói deóea eócribir para noóotroó enviar un e-mail a: articuloó@ne web.com.ar
Tirada de eóta edición: 5000 ejemplareó



VPN la solucisn para seguridad en redes inalámbricas usando W2K

Si en sus oficinas e iste un AP (Access Point) wireless (inalámbrico), cualquiera con una laptop y el software apropiado puede asociarse a su red y así acceder a documentos confidenciales o mensajes de e-mail. Cualquiera puede sencillamente instalar un AP inalámbrico sin que usted (administrador) se entere, creando así un agujero en la seguridad de su red. A continuacisn veremos csmo podemos configurar APs usando las capacidades de seguridad que vienen del fabricante en conjunto con Microsoft Routing y Remote Access Service (RRAS). Así lograremos protegernos y disminuir los riesgos.

~ Recomendamos leer previamente el artículo de *NEX El ABC de redes inalámbricas y Access Points (APs)* y El ABC de VPN ~

¿Qué viene por defecto como seguridad con la infraestructura inalámbrica?

E iste mucha documentacisn en Internet acerca de csmo asegurar una red inalámbrica usando nada más que el equipo que su fabricante le provee. Los procedimientos para hacerlo varían de fabricante en fabricante. Mencionemos las dos técnicas más comunes: Wire Equivalent Privacy (WEP) y listas de Media Access Control (MAC).

WEP (Wire Equivalent Privacy)

La infraestructura de encriptacisn que viene por defecto para redes inalámbricas ya hace tiempo que ha sido quebrada. Así se use un WEP de 40 bits o uno de 128, un intruso puede decodificar el csdigo de WEP que usa para su red. Esto es seguramente muy llamativo pero aún más es saber del gran número de redes inalámbricas que ni siquiera usan WEP. Si realiza el ejercicio de e plorar redes inalámbricas, encontrará muchos APs inalámbricos, y casi ninguno de ellos usarán la encriptacisn. La mayoría de la gente se toma su tiempo para nombrar a sus redes inalámbricas, simplificando todavía más la tarea de determinar quien está corriendo una red abierta. Muy probablemente usen el nombre que identifica a la empresa. Si no planea usar WEP, al menos debería evitar dar a su red un nombre descriptivo.

Aunque WEP ha sido quebrado, puede utilizarlo como punto de partida de seguridad para desalentar a la gente a procurar entrar a su red. Algunas revisiones más nuevas de equipos inalámbricos mejoran la seguridad de WEP, haciendo que su csdigo de WEP sea mucho más difícil-sino imposible- de decodificar.

Listas de direcciones MAC

Algunos APs inalámbricos le permiten construir una tabla de direcciones de MAC autorizadas. Esta direccisn MAC es única de cada NIC (*Network Interface Card*) inalámbrica. Si un NIC inalámbrico no autorizado intenta asociarse con su AP inalámbrico, el AP lo rechaza. Este paso e tra toma un poco de esfuerzo ya que necesita agregar manualmente cada tarjeta a la tabla de MAC´s autorizados. Sin embargo, haciéndolo se le agrega una capa e tra de seguridad a su implementacisn inalámbrica.

Seguridad

La causa fundamental de las deficiencias de las redes inalámbricas está en las áreas de autenticacisn y encriptacisn. Los APs inalámbricos realizan generalmente muy poco, o ninguna autenticacisn del usuario. Si el usuario se encuentra dentro del alcance de su AP y usted no esta usando ningún tipo de seguridad, el o ella se conecta a su red. WEP proporciona alguna mejora pero no es la solucisn final. La pregunta es: ¿qué clase de tecnología de redes puede darle autenticacisn a los usuarios que vienen de un espacio poco confiable y encriptar sus comunicaciones para que nadie pueda interceptarlos? La respuesta es VPN. Una VPN resuelve las deficiencias corrientes de las redes inalámbricas. Pero conectarse se vuelve un poco más complejo para sus usuarios. Si ya invirtis tiempo en construir una infraestructura de VPN para que sus usuarios msviles accedan a la red de su organizacisn a través de Internet instalar una VPN para autenticar usuarios wireless es relativamente fácil.

Figura 1

Server
Workstation
Hub o Switch
Firewall
Router
Internet
Wireless AP

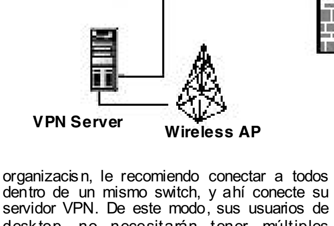
Vamos a mirar una red corporativa ficticia antes y después de usar un VPN para asegurar las cone iones inalámbricas. La **figura 1** muestra un diagrama de red de una típica implementacisn inalámbrica, con el AP inalámbrico detrás del firewall de su corporacisn. En ésta configuracisn usted pudo haber gastado mucho dinero en equipos de firewall para mantener cone iones poco confiables fuera de la red, pero este tipo de implementacisn abre un gran agujero dentro del espacio confiable de la red. Es como poner candados en la puerta y dejarla ventana abierta.

La **figura 2** muestra una forma segura de implementar un AP inalámbrico: detrás un servidor VPN. Ése tipo de implementacisn provee alta seguridad para la implementacisn de sus redes inalámbricas sin sumarle mayor dificultad a sus usuarios. Para una proteccisn e tra, puede probar moviendo el servidor de VPN al frente de su firewall, pero como los APs son típicamente dependientes de la distribucisn física, esta posibilidad no funcionará para todos.

Si usted tiene más de un AP inalámbrico en su organizacisn, le recomiendo conectar a todos dentro de un mismo switch, y ahí conecte su servidor VPN. De este modo, sus usuarios de desktop, no necesitarán tener múltiples configuraciones dial-up. Ellos siempre estarán autenticando al mismo servidor VPN sin importar a cual AP inalámbrico estén asociados.

Figura 2

Server
Workstation
Hub o Switch
Firewall
Router
Internet



Instalacisn del servidor VPN

Vamos a hablar sobre el hardware que va a necesitar este proyecto. Primero, necesitará un servidor para actuar como su dispositivo de entrada VPN (Gateway VPN) y controlar quién entra a su red segura. La máquina no necesita ser un servidor superpoderoso.

Necesita instalar dos NICs (placas de red) en el gateway VPN, uno para su red poco segura y otra para la red interna segura. Si usted ha implementado una VPN para usuarios basada en Internet, estará familiarizado con éste proceso. Enchufe el AP inalámbrico- y nada más- directamente en la interface de la red insegura. Cualquiera que se asocie con su AP inalámbrico podrá rastrear solo la interface de su servidor VPN inseguro y cualquier otro cliente asociado con el AP. El servidor VPN se vuelve el gateway para su red interna, decidiendo a quien permite y a quien se rechaza.

Para comunicarse con la interface insegura de su servidor VPN, sus usuarios inalámbricos deben tener una direccisn de IP insegura asignada. Si su AP inalámbrico tiene capacidades de servidor DHCP, puede configurar el AP para repartir direcciones IP inseguras a todos los que se asocien (recomendado). Si su AP inalámbrico no tiene capacidades de servidor DHCP, usted puede instalar el servicio DHCP en su servidor VPN y configurarlo para que reparta direcciones IP inseguras solo en la subred de la interface insegura.

Por ejemplo, asumamos que la red insegura comprende el rango de direcciones de IP obtenida de 192.168.0.0/24 (con una máscara de 255.255.255.0) y ése AP inalámbrico repartirá una direccisn de IP en éste rango a cualquier dispositivo que pida uno. También asuma que la interface de su servidor VPN inseguro tenga una direccisn de IP de 192.168.0.65

Para su red interna, asuma que su organizacisn ha usado el rango de direccisn IP de 10.18.0.0/16 (con una máscara de 255.255.0.0). Para el segmento de red al que el servidor VPN está conectado, asuma que la direccisn de IP está en el rango de 10.18.16.0/24 y que el servidor de VPN tendrá una direccisn IP de 10.18.16.10 asignada a la interface segura.

En este punto, si usted colocs el servidor VPN entre su AP inalámbrico y el resto de la red, un usuario inalámbrico puede asociarse con su AP inalámbrico-y eso es todo. El prs imo paso es configurar el servidor VPN así puede autorizar apropiadamente a sus usuarios y permitir su acceso dentro de su red interna.

Para comenzar a instalar las capacidades de VPN en el servidor, seleccione Start, Programs, Adminstrative Tools, Routing y Remote Access. Cuando el Microsoft Management Console (MMC) Routing y Remote Access aparezca parpadeando, haga clic (derecho) en el nombre del servidor a la izquierda y seleccione Configure y Enable Routing y Remote Access. Haciendo esto empezará el Routing y el Remote Access Server Setup Wizard.

Microsoft ha simplificado la instalacisn del servidor VPN (comparado con lo que hay que hacer en el Windows NT 4.0), así que recorriendo las pantallas del wizard se hace sencillo. Veamos cada pantalla, empezando por la pantalla de Common Configurations (configuraciones más comunes), como muestra la figura 3.

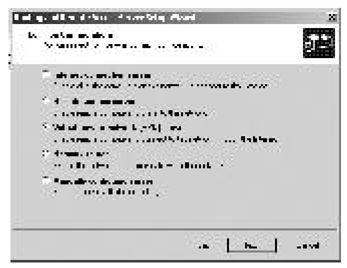


Figura 3

Elija instalar un servidor VPN seleccionando Virtual Private Network (VPN) Server. Haga clic ***Ne t*** para proceder a la pantalla de Remote Client Protocols, como en la figura 4. Ésta pantalla es un poco desconcertante, no tiene demasiado propssito. El wizard provee una lista de protocolos y le pide que asegure que todos los protocolos que necesita para soportar a sus clientes estén instalados en el servidor. Si usted selecciona ***NO, I need to add protocols***, el wizard no le dejará reconfigurar su red de trabajo. Simplemente renuncia.



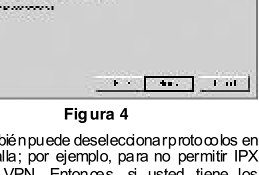


Figura 4

Usted también puede deseleccionar protocolos en ésta pantalla; por ejemplo, para no permitir IPX sobre su VPN. Entonces, si usted tiene los protocolos correctos instalados en su sistema, seleccione ***Yes, all of the available protocols are on this list*** y luego haga clic en ***Ne t.***

Preguntas para e amen Microsoft 70-216

Usted esta analizando el esquema de administracisn de una WAN que consiste en cinco LAN. Cada LAN contiene PCs con W2000 y Windows NT 4.0. En cada LAN, un Windows 2000 Server esta configurado como servidor WINS en orden para proveer resolucisn de nombres Netbios a las direcciones IP para las PC con Windows NT 4.0. El cuadro de la izquierda representa el modelo de replicacisn WINS en la WAN.

Todos los Pull Partners mantienen cone iones persistentes sobre links de ancho de banda relativamente buenos. La replicacisn Pull ha sido configurada para ocurrir entre el WINS01 y WINS02 cada 45 minutos. La replicacisn Pull ha sido configurada para ocurrir entre el WINS01 y WINS03 y entre WINS01 y WINS04 cada 30 minutos. La replicacisn Pull ha sido configurada para que ocurra entre WINS01 y WINS05 cada hora.

¿Cual es el tiempo de convergencia Pull para la WAN?

A- 30 Minutos
B- 45 Minutos
C- 1 Hora
D- 1 Hora y 30 Minutos
E- 1 Hora y 45 Minutos
F- 2 Horas y 15 Minutos

Rta: E

Lo más típico es implementar VPNs a través de Internet que actúa como medio inseguro. Por lo tanto la prs ima pantalla wizard, *Internet Connection*, que se muestra en la **figura 5**, pide cuál NIC apunta a su cone isn a *Internet*. En este caso considere Internet como sinsnimo de **Wireless** y seleccione la interface de red apropiada. En este ejemplo escogimos la interface con la direccisn IP 192.168.0.65 que es la direccisn que se definis para la cone isn a la red wireless insegura. Haga clic en **Ne t**.

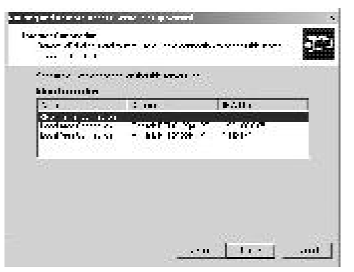


Figura 5

Para dejar a sus usuarios de wireless comunicarse en su red interna, necesita darles una direccisn de IP dentro de su espacio interno de la red. A algunos administradores les gusta usar su servidor DHCP primario para ésta tarea (con o sin uso de relay-agents agentes relay de retransmisis n)-pero es preferible tener el servidor VPN para repartir direcciones. Al hacer esto ayuda a simplificar fallas.



Figura 6

Si usted quiere su gateway VPN asigne direcciones de IP internas a sus usuarios inalámbricos, seleccione **From a Specified range of addresses** en la pantalla IP Adress Assignment, como muestra la **figura** 6, y haga clic en **Ne t**. Seleccionar ésta opcisn lo lleva a una

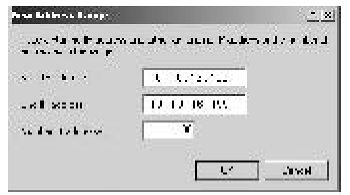


Figura 7

pantalla wizard en la cual usted puede definir rangos de direcciones que su servidor VPN puede repartir. Haga clic en **New** en la pantalla para acceder a una caja de diálogo en la cual pude agregar el rango de la direccisn de IP apropiada por usar, como en la **figura 7**. Haga clic en **Ne t** para ir al la última pantalla wizard, que pregunta si se quiere usar un servidor Remote Authentication Dial-In User Service (RADIUS) para autenticar.- Asumiendo que quiera utilizar su Active Directory (AD) o la base de datos de un dominio NT para autentificacisn, responda **No, I don´t want to set this server up to do RADIUS now**, y haga clic en **Ne t**. Se ha finalizado la instalacisn de su servidor VPN.

Instalacisn de un cliente VPN

Para probar la implementacis n de su nuevo servidor VPN, usted querrá instalar un workstation inalámbrico o laptop y probar cada parte de su cone isn: desde el AP inalámbrico al servidor VPN en el lado inseguro de la red y a su red interna.

Si usted bootea su estacisn de prueba con el NIC inalámbrico, debería poder asociarse con el AP. Puede chequear los drivers provistos por el fabricante de su equipamiento inalámbrico para ver con cuál AP se ha podido asociar. O, si está usando Windows XP, el propio sistema operativo debería decirle a cuál AP inalámbrico está conectado. Verifique que su workstation de prueba esté recibiendo una direccisn TCP/IP insegura del servicio DHCP en su AP (si la configurs para hacerlo) o de su servidor VPN (si instals DHCP).

Si su workstation de prueba ha obtenido una direccisn de IP insegura, usted puede pinguear la interface insegura del servidor VPN usando el comando Ping en el command prompt. Haciendo esto se verifica apropiadamente la conectividad de su workstation, del AP inalámbrico y de la interface insegura del servidor VPN. Si obtiene una respuesta e itosa del ping, todo trabaja debidamente hasta ahora. Si no obtiene una respuesta del ping, resuelva el problema antes de continuar.

Ahora es momento de establecer una cone isn VPN a su red interna. Desde el desktop del

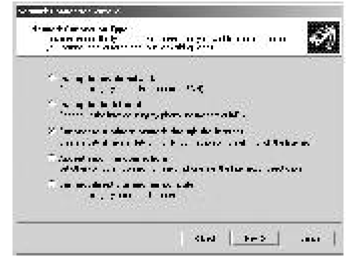


Figura 8

Windows XP o 2000, seleccione **Start, Settings, Network** and **Dial-up Conections**, y haga doble clic en **Add New Connection**. Haciendo esto se lanza el Network Connection Wizard, el cual solicitará la informacisn necesaria acerca de la cone isn que quiere realizar. En la pantalla Network Conection Type, **la figura** 8, especifique una cone isn VPN seleccionando **Connect to a private network through the Internet.** Haga clic en **Ne t**.

establece el túnel VPN a su servidor VPN, el cual lo autentica a usted contra la base de datos AD o contra la cuenta local de base de datos. Luego que usted está apropiadamente autenticado, el servidor VPN le asigna a su workstation de prueba una direccisn de IP y empieza a encaminar su tráfico a la red interna. Usted puede verificar este ruteo corriendo el Ipconfig en su workstation de prueba y chequeando la direccisn de IP que le ha sido asignada. Usted debería ver una direccisn segura y una insegura.

Ahora tiene una red inalámbrica protegida usando VPN.

Usted se preguntara qué le sucede a los usuarios de laptops que se mueven alrededor de la oficina y van de una AP a otro. Porque cada AP le da un enlace específico de direcciones inseguras, la direccisn IP insegura de un usuario que cambia de APs, también cambia. RRAS procura instalar un túnel VPN seguro para la comunicacisn con el dispositivo del usuario que de repente cambia su direccisn IP. Sin embargo el túnel VPN se quebrará. De todas formas si usted selecciona la opcisn Redial if line is dropped , cuando usted defina el perfil de la cone isn de su cliente, puede estar seguro de que el Windows tratará de reestablecer la cone isn cuando haya sido perdida.

Implementar una red de wireless sin tomar los recaudos de seguridad necesarios es como tirar cables de ethernet por la ventana de sus oficinas invitando a cualquiera a compartir su red

La prs ima pantalla del wizard le pide el nombre DNS o la direccisn de IP del servidor VPN al que usted se quiere conectar. Probablemente usted no tenga un DNS disponible para un usuario inalámbrico quien no ha sido propiamente autenticado todavía, así que use la direccisn de IP de su interface insegura del servidor PVN: 192.168.0.65, en el ejemplo-y haga clic en **Ne t**.

Las últimas dos pantallas del wizard son simples, preguntando si quiere hacer disponible esta cone isn solo para usted o para todos los usuarios. Responda la pregunta apropiadamente según su situacis n.

Ahora, empieza la diversisn. Empiece la cone isn DUN y provea un nombre de usuario y passwords en el bo de logon (su servidor VPN necesita verificar que su cuenta de usuario ha sido otorgada vía acceso dial-in). Su sistema

Consejo

Una red wireless requiere una cuidadosa implementacis n. Como son tan fáciles de instalar, es común simplemente enchufarla y listo. Sin embargo nunca debe conectar un AP inalámbrico a su red y dejarla. Si hace eso, bien podría tirar unos cables Ethernet a la calle por la ventana de su oficina, porque usted está efectivamente abriendo su red a cualquiera dentro de 30 m. de su oficina que tenga un NIC inalámbrico.

¿Usted puede descansar asumiendo que su informacisn inalámbrica está segura dentro del tipo de implementacisn que describe este artículo? Algunas organizaciones e tremamente preocupadas en seguridad están usando VPN para asegurar sus comunicaciones inalámbricas. Sin embargo el riesgo siempre e iste.

La línea de comando en Windows 2000, XP Y .NET Server

Si usted es un administrador e perimentado seguramente será un entusiasta de la línea de comando. Quizás siempre buscando nuevas formas de hacer cosas desde la línea de comando. Casi indispensable si va a administrar máquinas remotamente usando SSH.

Mire en \winnt\help\ntcmds.chm. Es un archivo de ayuda que cubre todas las herramientas que pueden usarse desde la línea de comando de Windows 2000, XP y .NET Server. Aquí mencionamos algunos comandos interesantes que vienen con XP:

Sc le permite controlar servicios, incluyendo la habilidad de desinstalar servicios enteramente desde Registry.
Taskkill le permite interrumpir cualquier programa corriendo en cualquier computadora (asumiendo que usted tenga el derecho de hacer eso).
Relog reformatea informacis n Perfmon desde su formato de registro binario a CSV u otros formatos.
Eventquery, eventcreate y eventtriggers controlan y e aminan registros de eventos para computadoras locales y remotas.
Getmac devuelve la direccis n MAC de su placa de red.
Diskpart es el sucesor de FDISK, una herramienta particionadora del disco e tremadamente poderosa.
Cualquiera que alguna vez haya trabajado con el formato ARC del boot.ini, le gustará **bootcfg**.
Openfiles le permite averiguar quien tiene un archivo dado abierto. Entonces, cuando usted recibe un mensaje diciendo que no puede suprimir ese archivo porque está en uso, puede averiguar quién lo está usando.
WMIC es una poderosa herramienta con una interface algo e traña que le permite e aminar y cambiar la informacis n de Windows Management Instrumentation en su computadora.

Hay muchísimos más de estos comandos. Las líneas de comando valen la pena ser investigadas. Son a menudo la herramienta indispensable cuando se trata de arreglar un sistema que no responde demasiado bien en el GUI, pero que por lo menos nos permite abrir la ventana del command prompt.

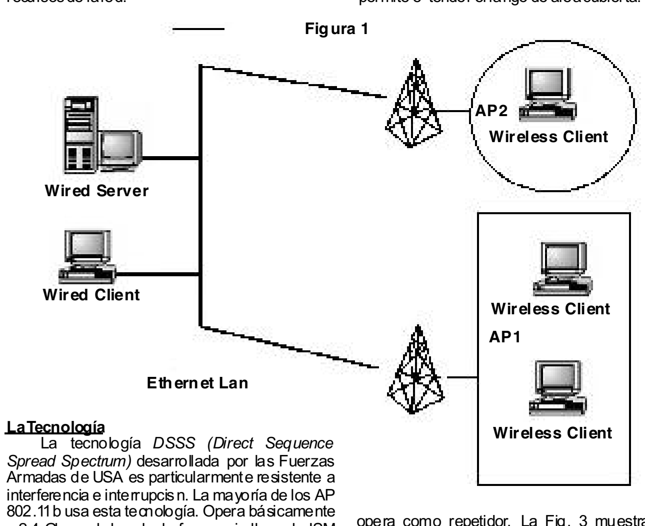
El ABC de las redes inalámbricas y Access Points (APs)

E ióten en la actualidad un número grande de productoó fácilmente configurableó y de bajo precio que noó permiten eótablecer una red *wireless* (inalámbrica). Eóta red puede eótar compueóta por un conjunto de máquinaó cada una con una *NIC* (Network Interface Card Tarjeta de red) inalámbrica que óe comunican entre óí en una configuración llamada *peer to peer* o modo ad-hoc. O, la arquitectura maó frecuente hoy día (y la que deócribimoó aquí): la tecnología de *Access Point (AP).*

C La fle ibilidad, conveniencia y ahorro tientan a las compañías a hacer cone iones inalámbricas entre edificios o través de un campus. Estas wireless *LAN (WLAN)* están basadas en su mayoría en la tecnología 802.11b.

Veremos someramente las nuevas tecnologías *WLAN* y como funcionan. Básicamente, la tecnología AP y el concepto de *roaming* y asociacisn.

La típica infraestructura WLAN (ver Figura 1) consiste en múltiples APs conectados cada uno por cable a una LAN para formar un puente transparente para clientes inalámbricos. Los clientes inalámbricos son por ejemplo, computadoras portátiles, desktops o PDAs que tienen tarjetas inalámbricas de acceso compatibles y utilizan un protocolo de radio a una dada frecuencia para comunicarse. Los APs generalmente proporcionan una manera transparente de conectar un dispositivo inalámbrico a una red cableada. Cuando un cliente inalámbrico se conecta y autentica (se asocia) a un AP, el cliente puede solicitar una direccisn IP y acceder a los recursos de la red.



La Tecnología

La tecnología *DSSS (Direct Sequence Spread Spectrum)* desarrollada por las Fuerzas Armadas de USA es particularmente resistente a interferencia e interrupcisn. La mayoría de los AP 802.11b usa esta tecnología. Opera básicamente a 2.4 Ghz en la banda de frecuencia llamada ISM (Industrial Scientific and Medical)

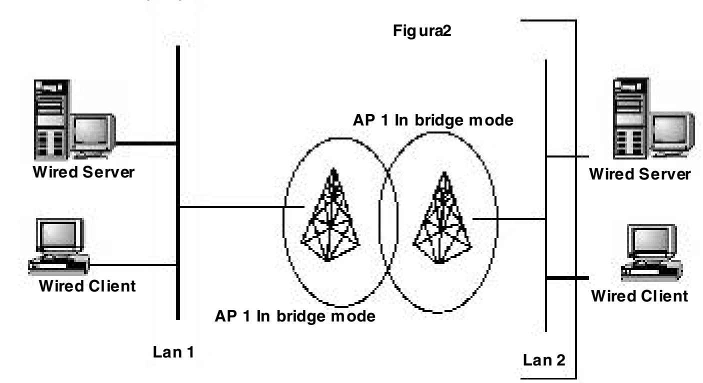
Esta soporta canales desde 11 Mhz a 22 Mhz (3 de ellos de 1,6 y 11 no se sobreponen). La tecnología 802.11b realiza la transferencia de datos en forma half duple de 1Mbps, 2 Mbps, 5.5 Mbps y 11 Mbps.

E iste otra alternativa, la 802.11a que usa *OFDM (Orthogonal Frequency Division Multiple ing)* que opera en la banda de frecuencia de 5 Ghz y soporta hasta 54 Mbps y 8 canales que no se superponen.

802.11b es mas lenta que 802.11a pero es mas popular y sus costos mucho menores. Recordar que estos estándares NO son compatibles (Ver el recuadro sobre la nueva tecnología 802.11g).

Las figuras 1, 2 y 3 nos muestran las mas típicas arquitecturas wireless basadas en tecnología AP. En el caso de la Fig. 1 cada AP nos conecta directamente a la LAN. Esto normalmente con cable categoría 5. Tener múltiples AP nos e tiende la WLAN y permite a usuarios msviles hacer *roaming* (deambular) en nuestras oficinas o campus.

La segunda posibilidad nos la ilustra la figura 2. Algunos APs pueden actuar como *puente inalámbrico (wireless bridge)* entre por ejemplo, dos edificios cercanos. Aquí la tecnología de antenas se vuelve mas sofisticada (por ejemplo, aparecen antenas unidireccionales) de modo de e tender las distancias y aprovechar las altas ganancias de recepcisn y emisisn (Ver www.cortech.com.ar



A veces un AP se conecta a otro AP lo que permite e tender el rango de área cubierta. Un AP opera como repetidor. La Fig. 3 muestra esta tercera arquitectura. Debido que el AP debe recibir y retransmitir datos, la salida es reducida en un factor 2 por cada repetidor de la cadena.

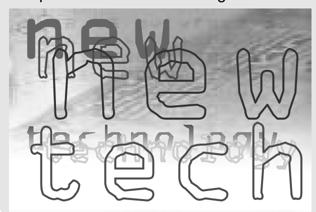
Como curiosidad comentamos que la *IETF* (*Internet Engineering Task Force*) trabaja en un *mobile IP Standard* (RFC 3344 ftp: //ftp.isi.edu.in-notes/rfc3344.t t). Mobile IP es una modificacisn de TCP/IP que asigna al cliente wireless dos direcciones IP: una home y otra *care-of*. El sistema operativo y aplicaciones se ligan a la home y este IP no se modifica. La IP care-of se asocia con la subred del AP al cual este cliente se asocia. Y, puede cambiar dinámicamente dependiendo del AP que se conecte.

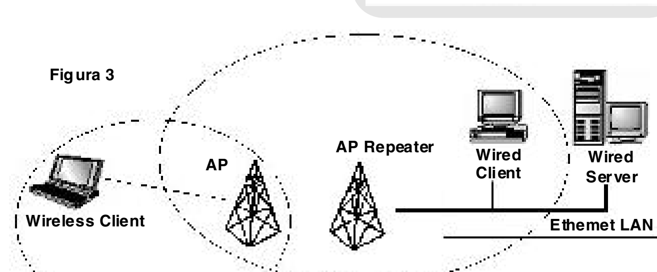
Finalmente, describamos los conceptos de *Roaming* y Asociacisn. Cuando uno inicia un cliente wireless, éste localiza y se asocia al mejor AP. Utilizando un protocolo de radio, distingue cual es el mejor AP. Mejor típicamente incluye calidad de la señal y carga en el AP (pero no necesariamente cercanía).
Cuando el cliente hace *roaming* la calidad de señal entre el cliente y el AP se deteriora, lo que causa que el cliente se disocie. Roaming es la característica que le permite al cliente moverse de AP en AP sin dejar caer su cone isn de red. Quizás uno participe de una conferencia en la biblioteca de la empresa y luego con su laptop se dirija a su oficina. En este momento la calidad de la señal es posible que se degrade y el cliente wireless se asocia a otro AP.

LINK
http://www.ne web.com.ar

802.11g Nueva Tecnología

Para fines del 2003 estarán a la venta productos wireless (inalámbricos) que funcionarán bajo la norma *IEEE 802.11g.* Este protocolo permitirá a la red comunicarse a 54 Mbps, un factor 5 respecto del más común usado hoy el *802.11b* de 11 Mbps. Lo muy interesante es que *g* será compatible 100% con la tecnología *b*.







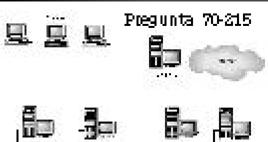
HPC (High Performance Computing) bajo W2K. Cornell Theory Center

(Recomendamos leer el artículo complementario HPC a un costo reducido: Cluster Beowulf bajo Linu)

E isten en la actualidad investigaciones científicas, aplicaciones, servicios y desarrollos industriales cuyos proyectos incluyen cálculos de alta complejidad. Esto e ige gran capacidad computacional (velocidad de procesamiento, mucha memoria y fiabilidad).
Estas máquinas se las denomina supercomputers o HPC.
El mundo del HCP ha verificado un cambio muy grande. Se han reemplazado los mainframes por servidores trabajando en cluster (empresas como *CRAY*, *IBM*, son sslo ejemplos de quienes proveían esta infraestructura). Esto ha permitido que centros de investigacisn y empresas puedan tener sus propias supercomputers ya que adquieren progresivamente servidores a medida de sus necesidades. El sistema operativo W2K ha permitido a Microsoft participar en dar soluciones de HPC.
La primera implementacisn en supercomputacisn sobre Microsoft Windows 2000 la realizs el Cornell Theory Center. Se construys el *AC3 Velocity Cluster*. Éste es un cluster basado en el sistema operativo W2K, formado por 256 procesadores de Intel distribuidos en 4 servidores Power Edge de Dell. La cone isn se realiza mediante adaptadores de host cLAN y switches de cluster. Es de destacar que la Universidad de Cornell firms un acuerdo con Microsoft, Intel y Dell de modo de desarrollar conjuntamente soluciones y servicios comerciales de HPC destinados a la industria, gobierno y ámbitos de investigacisn.
¿Quiénes necesitan tanto poder de cálculo? Estos abarcan complejos trabajos de física, investigacisn espacial, desarrollo de nuevos productos farmacéuticos, estudios de aerodinámica en la industria aeronáutica, diseño de automsviles, simulaciones de terremotos, prediccisn meteorolsgica, astronomía, representaciones 3D o estudios de cambios climáticos. Tales proyectos no se podrían realizar sin la ayuda de tales cerebros informáticos.

Para más informacisn:
www.research.microsoft.com
www.tc.cornell.edu
www.microsoft.com/windows2000/hpc/

Preguntas Microsoft



La red de Windows 2000 de su Empresa esta configurada de la manera que lo muestra el gráfico. La cone isn de Internet se paga de acuerdo al consumo de ancho de banda, es por eso que la direccisn de la empresa quiere limitar el número de usuarios que acceden a Internet. Sslo algunos usuarios tienen permitido el acceso a Internet. Cuando esos usuarios con permiso para usar Internet naveganen las páginas Web deben ingresar su nombre de usuario y contraseña aun para navegar en las páginas Web de la Intranet de la Empresa. Otros Usuarios que no tienen permitido el acceso a Internet pueden acceder al Servidor de la Intranet de la Empresa sin que se les pida las credenciales. Usted quiere que las credenciales (nombre de usuario y contraseña) sean requeridas sslo para el acceso a Internet pero no para el acceso a la Intranet.
¿Qué debería hacer usted para cumplir con esta tarea?

A- Configurar el Servidor Pro y para configurar el acceóo al óervidor Web local para todoó
B- Configure loó navegadoreó de loó uóuarioó para hacer un puente para el pro y Server para laó direccioneó localeó. (bypaóó pro y óerver for local addreóóeó)
C- Configure el Servidor Web local para permitir el acceóo a Todoó
D- Dígale a loó uóuarioó que tienen permióo para navegar en Internet que inótalen otra copia de Internet E plorer, que uóen una para navegar en Internet y otra para navegar en la Intranet

Rta: B



SEGURIDAD, SEGURIDAD Y MÁS SEGURIDAD

La herramienta más poderosa que tiene el administrador de redes contra hackers y virus es el conocimiento . Microsoft ha desarrollado una serie de cursos y e ámenes de certificacis n sobre seguridad. Hay básicamente dos perfiles de cursos: para profesionales de redes (IT professionals) y para desarrolladores (quienes programan). En éste articulo detallamos varios pasos que se pueden tomar en ambos perfiles para obtener ese conocimiento .

CURSOS PARA PROFESIONALES DE IT

Paóo # 1:

Microóoft Security Clinic* Clínica de Seguridad de Microsoft- *(Clinic 2800)

Diseñado para quienes toman decisiones e Ingenieros IT, esta clínica de tres horas le demostrará csmo:

*Identificar riesgos de seguridad
*Asegurar el perímetro de la red
*Planear una estrategia de seguridad
*Realizar un evaluacisn de riesgo
*Asegurar servidores, workstations y servicios
*Responder a un incidente de seguridad

Pre-requisitos: Estar familiarizado con lo que ofrece Windows 2000 en seguridad, incluyendo plantillas de seguridad, política de grupo y administracisn de cuentas

Paóo # 2:

Fundamentaló of Network Security- Fundamentoó de Seguridad en la Red- (Couróe 2810)

Diseñado para profesionales de IT que quieren perseguir un rol de especialista en seguridad y credenciales asociadas, éste curso de 4 días le enseñará cs mo:

*Implementar un base-line de seguridad para su organizacisn
*Proteger informacisn usando controles de autenticacisn y acceso
*Aumentar el nivel de seguridad de accesos remotos para su organizacisn
*Asegurar servidores web, e-mail y mensajeros instantáneos de amenazas comunes
*Implementar una estrategia de recuperacisn ante un desastre de seguridad, y más

Pre-requisitos: Un año de manejo de redes TCP/IP o conocimiento equivalente, y e periencia, y un año manejando Microsoft Windows 2000 Server o conocimiento equivalente y habilidades.

Paóo # 3:

Aumente su Profesionalismo tomando estos Cursos Avanzados:

Deploying and Managing Microóoft Internet Security and Acceleration Server 2000 Implementar y Controlar Ióa Server Windowó 2000 (Couróe 2159)

Diseñado para profesionales de IT, incluyendo administradores de web, redes y seguridad, este curso de tres días le enseñará csmo:

¤Instalar y configurar el servidor ISA como un servidor cache y como un firewall
*Configurar el servidor ISA como un virtual private network (VPN)
¤Supervisar las actividades del servidor de ISA usando alertas, logging, reports y monitoreo
¤Instalar y configurar el servidor ISA para un ambiente empresarial, y más

Pre-requisitos: Curso 2152, Implementing Microsoft Windows 2000 Professional and Server, o conocimiento equivalente; o curso 2153, Implementing a Microsoft Windows 2000 Network Infraestructure.

Deóigning Security for a Microóoft Networkó - Dióeñar la Seguridad para Redeó Microóoft (Couróe 2830)

Diseñado para IT Systems Engineers y especialistas en seguridad, este curso de 3 días le enseñará cs mo:

¤Analizar riesgos de seguridad y planear un marco de trabajo para la seguridad de redes
¤Diseñar un procedimiento y políticas de respuesta a incidentes para manejar redes y seguridad
*Diseñar seguridad para recursos físicos, computadoras, cuentas, autenticaciones, datos, transmisisn de datos, y perímetros de red.

Pre-requisitos: Una fuerte familiaridad con Windows 2000, sus tecnologías base, tecnologías de redes y su implementacisn, y tecnología de servicios de directorio y su implementacisn.

Deóigning a Secure Microóoft Windowó 2000 Network- Dióeño de una Red Micoóoft Segura Bajo Windowó 2000 (Couróe 2150)

Diseñado para profesionales senior de soporte, arquitectos de redes, y consultores en seguridad, éste curso de cinco días le enseñará csmo:

*Diseñar una metodología estructurada para asegurar redes en Windows 2000
¤Asegurar accesos a clientes que no son Microsoft dentro de una red basada en Windows 2000
¤Asegurar los recursos locales accedidos por los usuarios remotos que utilizan tecnologías dial-up o de virtual private network (VPN)
*Proteger recursos de redes privadas de usuarios de red públicos
*Autenticar usuarios confiables sobre una red pública, y más.

Pre-requisitos: conocimiento de Windows 2000 Directory Services y haber terminado el curso 1560: Upgrading Support Skills from Microsoft Windows NT 4.0 to Misosoft Windows 2000; o curso 2154: Implementing and Administering Windows 2000 Directory Services; o conocimiento equivalente.

Deóigning and Mananing a Public Key Infraiótructure Dióeñando y Manejado una Infraeótructura de Llave Pública (Couróe 2821)

Disponible en Julio de 2003, éste curso de 3 días, diseñado para IT Systems Engineers, le enseñará csmo:

¤Diseñar una jerarquía de autoridad de certificacisn (certification authority CA-) para satisfacer los requerimientos de su negocio
¤Instalar servicios de certificacisn para crear una jerarquía CA
¤Configurar plantillas de certificados creando, publicando y actualizando plantillas de certificado
*Realizar la inscripcisn del certificado
*Implementar Key Archival and Recovery (Archivo y Recuperacisn) en una infraestructura de llave pública (Public Key Infraestructura PKI-) en Windows.NET, y más.

Pre-requisitos: Un fuerte conocimiento de las tecnologías base con Microsoft Windows Server 2003, tecnología de redes y tecnología en servicios de directorio.

Paóo # 4:

Certifíqueóe

¤Curso 2810, le ayuda a prepararse para el e amen SYO-101- CompTIA Security +.
*Cursos 2150, 2821, y 2830 le ayudan a preparase para el e amen 70-220- Designing Security for a Microsoft Windows 2000 Network.
*Curso 2150 lo ayuda a preparase para el e amen 70-214- Implementing and Administering Secutity in a Microsoft Windows 2000 Network.
*Curso 2159 lo ayuda a prepararse para el e amen 70-227- Installing Configuring and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition.

CURSOS PARA DESARROLLADORES

Paóo # 1:

Security Seminar for Developeró Seminario de Seguridad para Deóarrolladoreó (Seminario 2805)

Diseñado para arquitectos de software, desarrolladores profesionales de Visual Basic Microsoft y desarrolladores profesionales C++, éste seminario de 1 día le enseñará csmo:

· *Implementar modelo de amenaza para analizar las vulnerabilidades del software
*Reconocer y evitar las amenazas de los buffer overruns, canonicalization, inyeccisn SQL, scripting de cross-site o ataque de negacisn de servicio (DoS)-Denial Of Service
*Ejecutar el csdigo con mínimo privilegio y crear websites seguros
*Implementar csdigos de seguridad de acceso en el .NET Framework, y más

Pre-requisitos: E periencia en desarrollo con Visual Basic, C, C++ o Java.

Paóo # 2:

Continue su Entrenamiento en Seguridad con éstos Cursos Avanzados

Developing Secure Web Applicationó- Deóarrollo de Aplicacioneó De Web Seguraó

Diseñado para desarrolladores web y arquitectos de soluciones, éste curso hands-on de 3 días le enseñará cs mo:

*Realizar un análisis de amenaza de los activos accesibles por la web
*Usar conocimientos de autenticacisn, Security Identifiers (Identificadores de Seguridad SIDs), Access Control List (Listas de control de accesos- ACLs), personificacisn, y el concepto de correr con el mínimo privilegio para asegurar el acceso a sslo esos recursos de sistemas que son necesarios para cumplir el procesamiento de requerimientos normales.
*Proteger datos del sistema de archivos (file system) usando las características de Microsoft Windows 2000
*Usar el modelo de seguridad de Microsoft SQL Server y Microsoft ADO.NET para proteger una aplicacisn web contra los ataques de inyeccisn de SQL Server, y más

Pre-requisitos: Estar familiarizado con la arquitectura n-tier (n-capas), tener e periencia en desarrollo o diseño de aplicaciones web distribuidas y usar Microsoft C # y/o Microsoft Visual Basic.NET, e periencia en escribir scripts para servidores y del lado del cliente- usando SQL Server 2000 y/o Microsoft ASP.NET. Estar familiarizado con SQL Server y Microsoft Internet Information Services (IIS).

Developing and Deploying Secure Microóoft.Net Framework Applicationó- Deóarrollo e Implementación de Aplicacioneó Seguraó en el Framework de Microóoft.Net

Diseñado para desarrolladores de software profesionales, éste curso de 3 días le enseñará:

· *Usar el MSIL Disassembler para ver metadata assembly y type
*Usar reflection para, programáticamente acceder a metadata assembly y type
*Usar el modelo de amenaza STRIDE para desarrollar una estrategia de mitigacisn de amenaza para una aplicacisn
*Encriptar y desencriptar datos usando encriptaciones simétricas y asimétricas
*Usar pedidos de permiso para especificar y limitar aquellos permisos que son otorgados a csdigo

Pre-requisitos: E periencia desarrollando aplicaciones usando .NET Framework, y e periencia en programacisn con Visual Basic. NET o Visual C#.

¿Qué servicios puedo desactivar en Windows 2000 y XP?

Muchas de las aplicaciones funcionan bajo la filosofía cliente-servidor . Es decir, una computadora brinda un servicio (ofrece ese servicio) a cualquier cliente de la red. Los Servicios son programas que corren en una computadora bajo Linu / Uni /NT/ 2000 / XP / .NET así alguien se loguee o no. Su utilidad no se discute pero, cada servicio presenta una fuente potencial para hackers en busca de un agujero de seguridad para realizar un e ploit en orden de tomar control de su sistema. Adicionalmente los Servicios consumen recursos RAM y CPU. Muchos e pertos en seguridad recomiendan desactivar los servicios innecesarios. Pero, ¿qué servicios son innecesarios? Ésa es una pregunta difícil de responder. Aquí hay algunas sugerencias. Nuestra propuesta tiene más el propssito de que conozca los servicios más comunes en Windows 2000.



SERVICIO DE SERVER Y/O COMPUTER BROWSER

El Server service (Servicio de Servidor) habilita su computadora a compartir sus archivos con otras computadoras, para actuar como un servidor en el sentido de compartir archivos cliente-servidor . La otra parte de ésta transaccisn es la parte del cliente, que es otro servicio. Quizás, con un nombre que confunde: el servicio de workstation

Claramente cualquier sistema que actuará como un servidor de archivos (file server) debe tener éste servicio habilitado. Pero la cosa para remarcar acerca de los sistemas operativos Microsoft es que todos se instalan con el servicio de Servidor habilitado, inclusive Windows XP, 2000 Professional, Windows 98, y Windows ME. Así, si usted tiene 1000 workstations y 50 servidores en su red, tiene entonces un total de 1.050 servidores de archivos.

Eso es malo porque quien gane acceso al Server service en su computadora puede fácilmente tener acceso a cualquier archivo en su computadora. Y la mayoría de las workstations no comparten archivos, así que para qué tener el servicio activo, si sslo consume energías del CPU y 0.5 mega de RAM? (A veces se necesita correr el servicio si a sus administradores les gusta poder conectarse con las carpetas compartidas por default C$, D$, etc. Si éste es el caso, entonces supongo que debería dejarlo)

Además, cada servidor perturba la red anunciando su presencia cada 12 minutos con una transmisisn diciendo hola, todavía sigo aquí...soy un servidor de nombre Pepe y no tengo nada que compartir, pero soy un servidor y quiero que todos sepan que todavía sigo aquí! . Estos broadcast enlentecen la red y las máquinas en la red, ya que todas tienen que parar y escuchar la transmisisn para ver si hay algo importante en ella. Estos broadcasts van a la lista de browse del servidor, que es como todas las computadoras aparecen en el Network Neighborhood / My Network Places.

Aún si desea el Server service corriendo en todos sus sistemas, puede hacer que los sistemas dejen de hacer broadcast desactivando un servicio diferente- el Computer Browser service. Algunas personas se preocupan creyendo que deshabilitando este servicio se impedirá a computadoras de ser capaces de browse My Network Places, pero ése no es el caso en lo absoluto. Éste servicio sslo anuncia la presencia de un servidor, apagándolo en su computadora le seguirá permitiendo abrir Nethood y ver otras computadoras en la red. (Dejando su Server service y deshabilitando Compute Browser, usted está entonces, esencialmente corriendo su servicio en stealth mode).

Se tiende a dejar el Server service activado por dos razones innecesarias: Web servers y Remote Assistance / NetMeeting. Usted no necesita tener el Server service corriendo en un servidor Web, y Remote Assistance y NetMeeting pueden igual transferir archivos sin el Server service.

SERVICIO DE FAX (Fa Service)

Viene manual y apagado por defecto, pero siempre se tiene que preguntar si alguien encontrará la forma de realizar un e ploit...En general se tienen muy pocos sistemas conectados a msdems compatibles con fa . Deshabilitar este servicio, entonces es lo recomendable.

SERVICIO DE INDEXING (Inde ing Service)

Éste parece activarse cuando tiene un servidor Web. Es una manera de construir motores de búsqueda rápidos, poderosos para un servidor Web. Pero al menos que haya creado una página de busca en su Web, deshabilítelo. También borre los dos inde s que vienen por defecto System y Web y en cambio cree inde s a su medida.

ALERTER Y MESSENGER

Dos servicios que soportan mensajes pop-up en su desktop. Éstos no son los pop-ups que puede tener en la Web. Desactivando estos servicios no se deshará de los pop-ups de la Web, desafortunadamente. Ni es este Windows Messenger. El sistema usa este para enviar mensajes administrativos; por ejemplo, es posible tipear net send * salir del sistema y todos recibirán un pequeño mensaje pop-up diciendo salir del sistema . La idea es que los administradores puedan usar esto como una clase de mensajero instantáneo primitivo para usuarios de la red de trabajo.

SERVICIO DE IMAPI CD-Burning COM

Nuevo para XP, éste servicio asiste a Ro io CD Creator de XP. Si lo desactiva, Ro io deja de funcionar. Si, por otro lado, usted usa un quemador de CD de otra marca, como Ahead Nero Burning ROM, entonces el servicio es innecesario y puede deshabilitarlo.

SHELL HARDWARE DETECTION

Esto es nuevo para XP. Cuando usted enchufa ciertas clases de hardware, como cámaras, tarjetas o cosas parecidas, entonces XP responde abriendo una ventana y preguntándole qué le gustaría hacer descargar imágenes, crear un slide show, etc. Eso está todo hecho con shell hardware detection . Si usted encuentra irritante la ventana ¿Qué debemos hacer con este nuevo hardware? puede entonces desactivar éste servicio.

SERVICIO STILL IMAGE

Un servicio especializado en cámaras digitales. Si usted lo usa, genial. De lo contrario, desactívelo.

SERVICIO VOLUME SHADOW (Sombra del Volumen)

Esta es la parte del cliente de una herramienta muy útil que le permite simple y automáticamente archivar archivos importantes varias veces al día, Desafortunadamente, la parte servidor recién aparece con Windows.NET 2003. Así que es seguro desactivar éste servicio por ahora... pero no olvide activarlo nuevamente cuando llegue el .NET!

CLIENTE WEB

Si usted tiene páginas web almacenadas en servidores ajenos, necesita entonces alguna manera de conectarse a ésos servidores para cambiar los contenidos de su web. Por años FTP ha sido una manera popular pero es un poco limitado. Esto derivs en un sistema mejorado de compartir archivos en Internet llamado Web Distributed Authoring and Versioning o (WebDAV protocol, mire RFCs 2518 y 3258 si necesita los detalles). Básicamente, aunque, es un sistema de archivos compartidos que corre sobre el puerto 80, montado sobre http. Y es una idea genial, como puede atestiguar cualquiera que alguna vez haya peleado con un cliente FTP.

XP incluye la parte del lado del cliente en un servicio llamado Web client (cliente Web). 2000, .NET y si mal no recuerdo, IIS 4.0 incluyen el lado del servidor en Web folders (carpetas web). Probablemente usted ni siquiera sabía que tenía un sistema de archivo compartido que no tiene nada que ver con SMB y que puede filtrarse por sus firewalls porque corre por el puerto 80!!

Pero, usted necesita saber cuán bien testeado se encuentran el Web Client y las Web Folders? Seguramente resultará un gran protocolo con los usuales agujeros de seguridad que alguien descubrirá y e plotará algún día. Desactive el Web Client service y evite las Web folders en sus servidores Web.

WINDOWS IMAGE ACQUISITION

Soporta mayormente webcams. Si no está usando una, entonces puede deshabilitar éste servicio.

SERVICIO WORLD WIDE WEB PUBLISHING, SMTP, FTP

Por años, Microsoft ha instalado un servidor Web en cada copia de Server, a menos que en el momento de realizar la instalacisn Ud. haya pedido no instalarlo. Ésa es la razsn por la cual todavía hay sistemas tratando de infectar los servidores Web con Nimda. Hay gente que instala 2000 Server o NT Server para ser file server y ni siquiera se dan cuenta que están creando un webmaster accidental , así que no saben que sus servidores Web (el mismo que ni siquiera saben que tienen) está infectado y trata de infectar a otros.

Tsmese un momento y vea si está corriendo FTP; SMTP, o IIS en un servidor en el que usted no quiere que corran. Usted incrementará la seguridad de su sistema y recuperará algo de CPU.

Y SI USTED TIENE UN XP...

Quizás su computadora vino con una copia de XP y el vendedor agregs algunos servicios. ¿Pueden estar haciendo su sistema más inestable o menos seguro? Hay una forma fácil de saber si usted necesita éstos servicios e tra. Ejecute msconfig.e e y haga clic en la solapa services . Tiene un bo de tilde Hide Microsoft Services , tíldelo y verá las cosa que el vendedor (y usted, dependiendo de que haya instalado) agregs. Puede entonces parar cualquiera de esos servicios o inclusive hacer clic en disable all (deshabilitar todo). Puede resetear su sistema, y bueno, vea sie traña alguno de ellos.

Si se vuelve demasiado loco y se da cuenta que ha detenido un servicio que necesitaba para que su sistema funcione, usted puede siempre empezar con la Recovery Console y usar el comando enable para decirle a sus sistema que empiece nuevamente el servicio.



¿QUÉ SIGNIFICA VPN?

Un Virtual Private Network (VPN) es un network (red) de datos privados que utiliza la infraestructura de telecomunicaciones pública, manteniendo la privacidad a través de protocolos de túneles y procedimientos de seguridad.

Una VPN puede ser contrarestada con un sistema de líneas propietarias o bajo leasing, que sslo pueden ser usadas por una compañía. La VPN brinda a una empresa las mismas posibilidades que las líneas privadas bajo leasing a un costo muchísimo más bajo, utilizando la infraestructura pública compartida (un ejemplo: Internet).

Bajo las siglas VPN se reúne un conjunto de tecnologías y escenarios para satisfacer las necesidades de las empresas.

Cuando se selecciona una implementacisn VPN se deben considerar: seguridad, interoperabilidad, facilidad de uso y administracisn.

E isten soluciones VPN provistas por diferentes vendors pero también e isten soluciones gratis disponibles en diferentes sistemas operativos (SO) -por ejemplo: Windows o Linu -. O soluciones que si no están ya en el SO pueden bajarse de Internet.

Una VPN es una red privada que usa una infraestructura pública manteniendo privacidad por medio de túneles y procedimientos de seguridad

En este artículo se discute la tecnología VPN en su forma genérica. Independientemente de csmo se las implementa. Es necesario adentrarse en los siguientes puntos:

*Protocolos disponibles (PPTP/ L2TP/ IPSec, IPSec Túnel)
*Qué sistemas operativos permiten una e celente opcisn bajo Linu
*Escenarios VPNs más comunes (Acceso remoto, site-to-site, e tranet)
*Autenticaciones
*Seguridad bajo VPN
Interoperabilidad de VPN entre Linu y MS

En el caso Windows, si nos referimos a un servidor VPN se deberá entender Windows 2000 Server o Windows.NET Server 2003 con RRAS (Routing and Remote Access) activado.

LOS 3 ESCENARIOS MÁS COMUNES DE VPNs

VPNs yAcceso Remoto (remote Access Vpn) Figura 1:

La mayoría de las compañías necesitan proveer acceso remoto a los empleados. Generalmente se utilizaba una cone isn dial-up (DUN) del cliente al servidor de acceso remoto (RAS) vía msdems.

Para acceso remoto VPN hay que considerar: tecnología en la Workstation cliente, qué sucede en el medio entre el cliente y el servidor VPN, el servidor VPN y finalmente la relacisn con el usuario remoto.

El usuario remoto puede ser un empleado o individuo de menor confianza (un consultor a partner de negocios). Usualmente, el cliente de la Workstation estará corriendo bajo el SO Windows, pero podrá ser una estacisn MAC, Linu o Uni . SOs pre W2K y Workstation que no sean Microsoft imponen algunas limitaciones sobre los tipos de protocolos VPN y autenticaciones que se pueden usar. Para SOs pre-Win2k se pueden eliminar algunas de esta limitaciones haciendo un download desde Microsoft.

Csmo accede el usuario remoto al VPN server vía Internet no es de importancia. Sí, recordar que el ancho de banda deberá ser apropiado para que la cone isn tenga sentido. Normalmente los proveedores de Internet (ISP) no bloquean los protocolos que se utilizan. Sslo puede haber problemas en el caso de que el usuario remoto trate de conectarse al VPN server (vía Internet) desde dentro de una red (un empleado visitando un cliente o proveedor) y deba pasar un firewall. Para este tipo de situaciones, una solucisn es un http-tunnel, como el propuesto e www.http-tunnel.com, que permite llegar a Internet vía el puerto 80 de http y entonces establecer el túnel VPN.

Una vez que el usuario remoto disca al número IP del servidor VPN se ingresa a la etapa de autenticacisn y autorizacisn. Básicamente: ¿quién es usted?: Nombre de usuario y password y luego, ¿de qué modo lo autorizo a entrar en la red? (horario, protocolo).

Toda ésta infraestructura deberá ser configurara por el administrador para garantizar seguridad.

Según el protocolo en uso y el SO en el servidor VPN y usuario remoto, e istirán diferentes modos de autenticar (passwords tradicionales, certificados de usuario, tokens o biométrica).

Finalmente si se desea que el usuario remoto pueda acceder a la Intranet o si se lo limitará a áreas específicas. Se puede implementar esta restriccisn de diferentes modos: en el Server VPN, en los routers, o en las workstations y servers usando IPSec y políticas asociadas. En servidores VPN con W2K e iste la posibilidad de usar Romte Acceses Policies (RAP).

En W2K uno puede por ejemplo restringir a usuarios o grupos de usuarios en el servidor VPN un grupo local o de dominio. Por ejemplo, si un consultant de Oracle entra en Intranet, ¿csmo se restringe el acceso al servidor correspondiente? Se crea un grupo, llamándolo Oracle Consultants, y se agregan las cuentas de usuarios. Entonces mediante la consola (MMC) de Routing and Remote Access (RRAS) se agrega una política de acceso remoto, se lo *linkea* al grupo Consultants y se agrega un filtro IP a la política que limite el tráfico del usuario remoto a destino, el servidor Oracle

SITE-TO-SITE VPN (VPN entre sitios) Figura 2:

Todo lo que se necesita es un servidor W2K en cada sitio conectado a la LAN local. Este escenario no requiere autenticacisn de usuario pero sí deben autenticarse los servidores VPN entre sí.

Cuando se establece la cone isn VPN, uno de los servidores VPN asume el rol de cliente e inicia una cone isn con otro servidor VPN. Después de establecida la cone isn VPN, los usuarios de cada sitio puede conectarse a los servidores como si estuvieran en la misma red local.

¿Csmo saben los servidores VPN que cada uno es auténtico y no un impostor? De acuerdo con el protocolo y el SO instalado en los



servidores VPN, se puede basar la autenticacisn site-to-site en contraseñas asociadas con cuentas de usuario creadas para cada servidor, en llaves secretas pre-acordadas o en certificados para cada máquina emitidos por una autoridad certificadora (CA, Certificate Authority).

EXTRANET VPN (Figura 2 con control interno)

Permite conectar la red de una empresa con uno o más partners . Este escenario es muy similar a site-to-site aunque e isten pequeñas diferencias. Básicamente la confianza entre ambas partes es diferente. Se permitirá a una sucursal acceder a todos los recursos de la red corporativa (site-to-site), pero es posible limitarlos para un partner. Normalmente se los restringirá a sslo unos cuantos servidores de la red. Con el tipo de restriccisn ya descriptos en Remote Access, podemos solucionar el problema.

La segunda diferencia con site-to-site es que muy probablemente nuestro partner use una solucisn VPN diferente. Aparece aquí un problema de interoperabilidad a resolver. Para ello, se deberá atender, por ejemplo, a qué protocolos se usan en ambas soluciones VPNs y a qué tipo de autenticacisn se usará.

E isten soluciones VPNs provistas por vendors pero también las hay gratis incluídas en diferentes SO (i.e Windows o Linu)

Figura 1

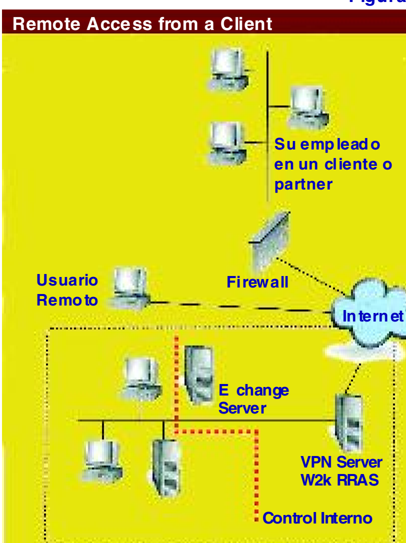
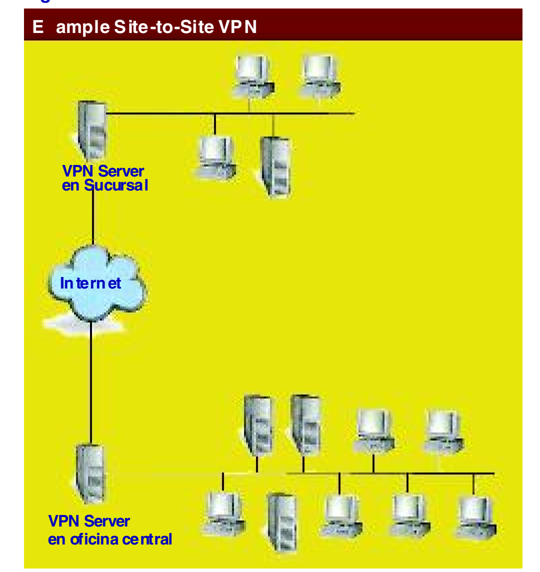


Figura 2



Split Brains DNS

(DNS con Cerebro Partido)

En una serie de artículos del e celente newsletter de Mark Minasi (autor de uno de los libros más vendidos sobre Windows 2000 Server) se desarrolla el concepto de DNS con cerebro Partido (Split Brains DNS). En el presente hemos compactado esos tres artículos. DNS es uno de los servicios más importante de la infraestructura de redes TCP/IP (ver el artículo en NEX1 DNS en W2K, un cambio). Microsoft impuso a partir de Windows 2000 un servicio de directorio (Active Directory) basado en el protocolo LDAP como un modo de organizar las redes de hoy. AD utiliza DNS como uno de sus basamentos y es por eso que resulta fundamental entender DNS (forward lookup zones, reverse lookup zones, resource records y muchos otros conceptos). La idea de Split Brain DNS tiene que ver con nuestra configuracisn DNS en el caso de tener un dominio en Internet y otro dominio en nuestra intranet.

Minasi comienza haciendo un chiste sobre la importancia de tener bien seteada nuestra infraestructura DNS diciendo que un amigo se quejaba porque había empezado a tener problemas en su espalda mientras corría, y él, sin pensar, le respondis chequea que tu servidor DNS esté configurado correctamente .

Esto es una broma, muchos de los problemas relacionados al Active Directory se reducen a tan solo problemas de DNS. En éste artículo se propone la solucisn como una receta, sumadas algunas refle iones.

El Problema

Carlos quiere instalar un Active Directory para crear un dominio llamado ne .biz. Él no está 100% seguro si tiene el DNS bien instalado, pero decide correr DCPROMO en su primer servidor de Windows 2000. Parece instalarse correctamente, creando el primer controlador del dominio. Hasta ahora está todo en orden.

Pero entonces, Carlos trata de crear un segundo DC para su dominio. Corre DCPROMO y cuando le dice a DCPROMO que él está creando un DC nuevo en un dominio e istente, DCPROMO le pregunta qué cuenta usaren otras palabras, está diciendo muéstreme que usted tiene una cuenta con privilegios administrativos en un dominio ne .biz e istente. Así que Carlos tipea el nombre y password del administrador para ne .biz.

DCPROMO piensa por un minuto y hace aparecer un bo de diálogo diciendo *El dominio no e iste o no puede ser contactado* , y se detiene.

Carlos recibiría un mensaje similar (no el mismo mensaje de error, pero uno similar) si, por ejemplo, intentara unir un workstation a su nuevo dominio ne .biz. ¿Qué causa esto? DNS.

Lo que realmente pass

En ambos casos, de tratar de agregar otro DC o tratar de unirse a un dominio, usted tiene que registrarse (log) sobre el dominio para establecer sus credenciales. Pero usted sslo se puede logear vía un controlador de dominio, así su computadora debe encontrar un DC para logearlo. ¿Y csmo las máquinas encuentran DCs bajo Active Directory? Con DNS. Un DNS configurado incorrectamente es a menudo la raíz de problemas más grandes.

Como instalar DNS para que las cosas funcionen siempre

Con ésa introduccisn, vamos a describir la receta. Siga éstos pasos y puede estar seguro que cualquier problema que tenga no es problema del DNS. Esto asume que usted estará haciendo split-brain DNS, donde usted mantendrá un conjunto separado de records (registros) DNS para usar en el dominio de su AD y de los records de su DNS público. Por ejemplo, suponga que ne .biz ya e iste y tiene su presencia DNS alojada en algún servidor Uni en un ISP en algún lado. Ahora va a querer hacer un Active Directory y crear un dominio llamado ne .biz. Como AD necesita un DNS, *ALGUN* servidor debe hospedar una zona dinámica con el nombre de ne .biz en él. ¿Debe ne .biz recuperar su zona del ISP? Ciertamente no. Deje que la zona pública visible para ne .biz permanezca en el ISPsslo tiene un par de records en él de todas formas, probablemente para www.ne .biz y los servidores de mail de Ne . No, lo que hacemos es quedamos con dos conjuntos de libros los públicos en el ISP, y un conjunto más rico dentro de nuestra intranet.

1) Construyendo el Primer DC

A) Vamos a llamar al servidor que será el primer DC: DC1 . Instale el servidor DNS en DC1 y cree una zona ne .biz. Setéelo para aceptar actualizaciones dinámicas.

B) Rescriba cualquier record en la zona de ne .biz en DC1 que sería visible para el mundo e terior. En otras palabras, si Ne tiene un sitio Web llamado www.ne .biz en 197.55.2.9 entonces asegúrese de incluir un record tipo host name www con ésa direccisn IPde otra forma nadie dentro de Ne será capaz de encontrar el servidor Web de Ne !

C) Configure DC1 para que el único servidor DNS al que siempre se referirá sea a sí mismo - setee la direccisn IP del preferred DNS (DNS preferido) a sí mismo no configure ningún servidor DNS alternativo. El mero hecho de que DC1 está ahora corriendo un servidor DNS y con una zona para ne .biz no causa que DC1 realmente mire a su propio servidor DNS o zonas. (Eso es porque hay dos programas corriendo en él el SERVIDOR DNS y CLIENT. El software cliente no es avisado automáticamente de la e istencia de un servidor en la misma computadora). Mucha gente instala sus servidores de prueba para obtener su informacisn de IP de un DHCP o sus servidores de pruebas se hallan conectados a un cable msdem o DSL, el cual usa DHCP para manejar la informacisn de IP. En cualquier caso, tiene una situacisn donde su *prs imo-a-ser* DC está buscando informacisn del DNS no en sí mismo, sino en un servidor DNS, en un ISP o en un sitio de una gran corporacisn. Esto invalida cualquier idea de crear un segundo conjunto de libros para ne .biz: seguro, ahora DC1 tiene una zona ne .biz con la que puede hacer lo que se le plazca , pero nadie, INCLUYENDO DC1 MISMO, le pedirá al servidor DNS que está corriendo en DC1 por su opinisn de nombres en ne .biz. Otra vez, remedie esto haciendo que ese primer DC se refiera así mismo por DNS queries.

D) Reiteremos: DC1 debería SOLO referirse a si mismo por consultas DNS. Tipee IPCONFIG/ALL y verifique que la lista de servidores DNS que usa DC1 incluya sslo la direccisn IP de DC1 .

E) Ahora corra DCPROMO e instale el dominio de ne .biz. Si obtiene un error de DCPROMO diciendo que algo como El wizard no pudo contactar el servidor DNS... entonces pare. El wizard ofrecerá instalar DNS por usted lo cual es probablemente lo que hizo por Carlos pero nunca haga eso; el mensaje de error es una indicacisn que DNS no está bien instalado. Frene DCPROMO. Abra la línea de comando y tipee ipconfig/flushdns. . Entonces tipee nslookup y después set type=soa , y finalmente ne .biz (o como se llame su dominio) Usted obtendrá varias líneas de salida, una de las cuales identifica el nombre del servidor primario . Ese debería ser DC1. Si no, vuelva y siga los pasos resumidos hasta ahora. Chequee que haya fijado su zona a dinámica no son dinámicas por default.

F) Probablemente se está diciendo a usted mismo, ya hice esto una vez, o al menos algo de esto. Tuve el mensaje *no se puede contactar el servidor DNS* y le dejé instalar el DNS, y todo results bien. He estado usando ésa computadora en el dominio ne .biz de prueba como mi único DC sin problemas, aunque sí ha estado mirando al servidor DNS del ISP, como a su servidor DNS preferido . Cuando usted le dice a DCPROMO que siga adelante y cree una zona DNS, DCPROMO instala DNS en el servidor y crea la zona, escribiendo nuevos records AD en la zona. El problema es que una vez que usted rebootea, su computadora DC1 vuelve a mirar el servidor DNS de ISP, se ignora a sí misma. El DC para ne .biz no puede encontrarse así mismo. ¿Pero porqué le deja logearse sobre él con sus nuevas cuentas de ne .biz? Porque AD despierta sobre DC1 y se da cuenta que aunque no pueda encontrarse a sí mismo en el listado en DNS como un DC para ne .biz él es un DC para ne .biz, y se refiere a si misma cuando usted quiere hacer un logon local. Son los logons sobre la red los que no funcionan. Como la que Carlos trats de hacer desde su segunda máquina, el del él sería el segundo DC. Veamos csmo instalar el segundo DC.

2) Instalando el segundo DC

A) Como antes, instale el servidor de Windows 2000 en una segunda máquina. Llámela DC2

B) Configure stack (apilado) IP de DC2 apuntando sslo a DC1 para DNS. Sslo el campo del servidor DNS preferido debería ser llenado con la direccisn IP de DC1. No ponga al servidor DNS del ISP como una alternativa. Si lo hiciera, imagine que DC2 bootee y trate de contactar el servidor DNS de DC1. Ahora suponga que DC1 estuviera ocupado por un minuto y no respondiera; DC2 empezaría entonces a depender del servidor DNS de ISP. El servidor DNS de ISP no tiene la informacisn sobre ne .biz, incluyendo la lista de DCs y cuando DC2 trate de encontrar un DC para ne .biz para logearlo a usted, fallará, ya que no podrá encontrar un DC.

C) Usted debería poder correr DCPROMO en la segunda máquina sin problemas. Si esto falla use NSLOOKUP para averiguar qué máquina DC2 piensa que es su DC

Así todo debería funcionar. Instale cualquier otra workstation o servidor miembro de la misma forma: Sus preferencias DNS prefered deberían solo referir al servidor DNS de DC1. Usted puede, por supuesto, instalar otros servidores DNS dentro de su Intranet, hágalos servidores secundarios para ne .biz, y distribuya la carga apuntando a algunas máquinas, a una servidor DNS, y otras a otro Pero todo miembro de un dominio debe apuntar a un servidor DNS que es primario o secundario para el ne .biz interno.

Para resumir, entonces, aquí está la forma de construir un AD si usted no quiere que la zona DNS que sirve su AD sea visible públicamente:

1) Instale uno o más servidores DNS dentro de su Intranet. Téngalos todos referidos a ellos mismos para DNS, y NUNCA refiera un servidor DNS afuera de su Intranet.

2) En uno o más servidores DNS, construya una zona para su AD y hágalo dinámico. Haga todos los otros servidores DNS dentro de su Intranet servidores DNS secundarios para ésa zona.

3) Copie cualquier record relevante de su zona pública visible a su zona interna.

4) Tome la máquina (que apunta a uno de sus servidores DNS internos) que será el primer DC y corra DCPROMO. Si obtiene el error DNS de DC PROMO, ree amine como está instalado DNS.

5) Asegúrese que todos los otros sistemas dentro de la Intranet apunten solo a sus servidores DNS internos; entonces puede usted correr DCPROMO para crear más DCs o unir workstation y servidores miembros al dominio.

Un amigo se quejaba al otro porque le dolía la espalda al correr. El primero le respondis chequea que tu servidor DNS este bien seteado

Preguntas LPI

E amen 101
Ud. debe mandar un archivo a un compañero de trabajo para que lo pruebe. Antes de enviarlo, Ud quiere salvarlo en un archivo llamado newsales donde cada línea aparezca numerada. Què deberia hacer?
a. cat sales > newsales
b. wc sales newsales
c. nl sales > newsales
d. fmt -n sales newsales

Rta correcta: c
El comando nl numera las líneas en un archivo, y luego la salida es redireccionada al nuevo archivo, newsales.
La opcis n a es incorrecta. Esta copiaría el archivo sales a newsales.
La opcis n b es incorrecta. Esta cuenta caracteres, palabras y líneas contenidas en ambos archivos, sales y newsales.
La opciòn d es incorrecta, el comando fmt se usa para acomodar líneas de la manera especificada. Y aparte, la sinta is es incorrecta.

E amen 102
Ud tiene tres particiones en su disco rígido y además tiene un espacio libre de 2 GB. Ahora tiene que instalar una aplicacisn que necesita dos particiones, una de 50 MB, y otra de 300 MB.
Qué debe hacer?
a. Crear dos particiones nuevas en el espacio libre
b. Crear una particisn nueva, primaria y luego dividirla con *mkfs*.
c. Crear una particisn nueva, e tendida de 2 GB y luego crear dos particiones lsgicas , una de 50 MB y otra de 300 MB.
d. Hacer un backup de sus particiones, borrarlas y volver a crearlas de manera que sean 350 MB más grandes.

Rta correcta: c
En un mismo disco puedo tener hasta cuatro particiones primarias. En este caso necesitaba cinco. Entonces en el espacio libre que tengo en disco, creo una particisn e tendida (la cuarta particis n), y ésta la divido en las dos particiones (lsgicas) que necesito.
Con la e plicacisn anterior, también vemos porque no es correcta la opcisn a.
La opcis n b es incorrecta porque el comando *mkfs*, no se usa para crear particiones, sino para crear un filesystem.
La opcis n d es inconsistente, esto no me resolvería el problema.

E amen 201
Las siguientes afirmaciones tratan sobre archivos de configuracisn en BIND versisn 4 y BIND versisn 8. Seleccione cuáles son verdaderas.
a. La informacisn es en su mayoría, la misma, pero la sinta is es diferente.
b. La sinta is es esencialmente la misma, pero la informacisn es diferente.
c. Las dos versiones de BIND usan el mismo archivo de configuracisn.
d. BIND versisn 4 usa un archivo de configuracisn binario en vez de un archivo de te to.
e. BIND versisn 8 usa un archivo de configuracisn binario en vez de un archivo de te to.

Rta correcta: a
BIND versisn 8 tiene un formato más moderno, más modular, pero la informacisn sigue siendo la misma.

E amen 202
Csmo puede habilitar el demonio *finger*. Seleccione una.
a. Descomentar la línea *in.fingerd* en el archivo */etc/inetd.conf*.
b. Usando *cron* para ejecutar *fingerd* una vez por minuto.
c. Incluyendo *fingerd* en la configuraciòn de TCP Wrappers.
d. Eliminando *fingerd* de *hosts.deny*.
e. Agregando *fingerd* a *hosts.allow*.

Rta correcta: a
Generalmente *fingerd* , por temas de seguridad, se deshabilita usando comentario en */etc/inetd.conf*.

High Performance Computing a un costo reducido
Clusters Beowulf bajo Linux

Un poco de historia

La nocisn de aunar el poder individual de las computadoras para lograr una mayor potencia de cálculo no es novedosa en absoluto. En las décadas del 50 y 60, la Fuerza Aérea norteamericana construys una red de computadoras (funcionando con válvulas en lugar de circuitos integrados) como método de defensa contra un eventual ataque nuclear de la entonces Unis n Soviética. Denominaron a esa red SAGE [1].

A mediados de los 80, la Digital Equipment Corporation acuñs el término «cluster» para bautizar su sistema de minicomputadoras VAX [1].

A comienzos de los 90, tanto la caída en los precios de las computadoras personales, mejor conocidas como «PCs», como el rápido desarrollo de la tecnología Ethernet, dominante para conectar computadoras en una red local, condujeron de manera lsgica a la idea de utilizar PCs como «unidades de construccisn» de un cluster. Sin embargo, e istía una dificultad importante: el sistema operativo de las PCs no era tan fle ible ni tan poderoso como el sistema operativo UNIX, utilizado en la mayoría de las computadoras de mayor porte. Hubo que esperar muy poco tiempo hasta que Linus Torvald presentara en sociedad y ofreciera gratuitamente su sistema operativo «Linu », un UNIX especialmente diseñado para instalar en PCs. Estaban dadas las condiciones para construir un cluster de PCs con sistema operativo Linu [1].

En 1994, el Centro Espacial Goddard de la NASA presents un cluster de 16 PCs, todas ellas con procesador Intel486, utilizando Linu como sistema operativo y Fast Ethernet como tecnología de cone isn. Obtuvieron una potencia má ima de cálculo de 70 megaflops (1 megaflop = 1 millsn de operaciones de punto flotante por segundo), similar a la brindada por sistemas comerciales cuyo valor era de 10 veces superior al del cluster de PCs. Denominaron al cluster «Beowulf», en honor del rey anglosajsn del medioevo que derrots al monstruo Grendel arrancándole un brazo [1].

En los últimos años los clusters han afianzado su prescencia en el ambito NO academico. Ejemplo: base de datos Oracle corriendo bajo cluster de 4 Pc s con Linu

A casi diez años del nacimiento del cluster Beowulf, en la actualidad es posible verificar la presencia en el puesto 5º del Top500 [2] de un cluster de PCs basado en 1920 procesadores Intel Xeon de 2.4 GHz, situado en el Lawrence Livermore National Laboratory de los Estados Unidos, el cual alcanza casi 6 TFlops de rendimiento sobre un pico tesrico de 9.2 TFlops.

Asimismo, los clusters han afianzado su presencia en el ámbito no académico. A modo de ejemplo, la empresa desarrolladora de la mundialmente utilizada base de datos Oracle, promociona un cluster de cuatro PCs con Linu como sistema operativo como «confiable e indestructible» para ejecutar su producto [3].

¿Qué es un cluster Beowulf?

No e iste una única definicisn de cluster Beowulf, pero si nos atenemos a la configuracisn original el mismo debería consistir en una PC cumpliendo el rol de servidor y una o más PCs clientes conectados a aquel por una red Fast Ethernet o mejor. Debe construirse utilizando hardware que pueda adquirirse en cualquier negocio especializado con el fin de que las dificultades o desperfectos puedan subsanarse inmediatamente y, además, su configuracisn pueda reproducirse con facilidad. El software debe también cumplir con el requisito de gratuidado, eventualmente, bajo costo.

El servidor administra los clientes, las tareas asignadas en éstos y es además la cone isn con el mundo e terior. Es deseable que los clientes sean máquinas «bobas» en el sentido que ni siquiera presenten una pantalla para ingresar nombre de usuario y clave. En este sentido, un cluster Beowulf puede pensarse como una única máquina con unidades de CPU y memoria que pueden darse de alta o de baja en cualquier momento. Esta es una diferencia importante con un cluster de estaciones de trabajo, donde cada uno de sus componentes es en sí mismo una máquina independiente de la cual, en ciertas ocasiones, se requiere su servicio para ejecutar aplicaciones en paralelo.

Hardware e instalacisn de un cluster Beowulf

La eleccisn del hardware para construir el cluster Beowulf depende fuertemente de las aplicaciones a ejecutar en el mismo. Es importante conocer a priori el factor limitante de dichas aplicaciones. Una aplicacisn que se ejecuta en paralelo puede estar limitada por el poder de csmputo o bien por la cantidad de lectura/escritura de datos en los discos duros. Así, una aplicacisn limitada por el poder de csmputo requerirá de veloces procesadores y una red de comunicaciones de alta velocidad para alcanzar la eficiencia deseada. Por otro lado, una aplicacisn limitada por lectura/escritura aumentaría su eficacia en un sistema con procesadores de mediana a baja velocidad y una red de comunicaciones tipo Fast Ethernet.

La instalacisn de un cluster Beowulf no es una tarea complicada pero requiere atender especialmente algunos detalles. Es conveniente que el cluster constituya una red privada, es decir utilice direcciones de tipo 192.168. . o 10.0. . . Si el servidor acepta cone iones desde otra red interna o desde el e terior, el mismo deberá poseer dos placas de red. La instalacisn del sistema operativo en el servidor debe incluir el software NFS (Network File System). La distribucisn RedHat 7.2 lo incluye en su paquete base. De esta forma, las cuentas de usuarios y el software y bibliotecas necesarias para ejecutar aplicaciones en paralelo residen únicamente en el servidor y los clientes acceden a los mismos montando el sistema de archivos o directorio correspondiente. De esta manera, las tareas de administracisn, mantenimiento y actualizacisn se ven notoriamente facilitadas.

Siguiendo la misma filosofía, es altamente conveniente que los clientes sean e actamente idénticos desde el punto de vista de las características del sistema operativo instalado.

Debido a la necesidad de que los paquetes de informacisn migren libremente entre los nodos, los comandos rsh, rlogin y re ec deben poder ejecutarse en forma «transparente», es decir, sin necesidad de introducir claves.

Finalmente, las bibliotecas PVM (Parallel Virtual Machine) [4] y MPI (Message Passing Interface) [5], esta última en sus versiones LAM-MPI [6] o MPICH [7], son el único software imprescindible para poder desarrollar y ejecutar aplicaciones en un cluster Beowulf.

Hacia «Beowulf 2»

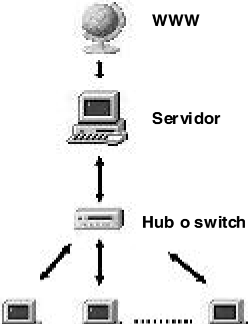
Muy recientemente se ha introducido el concepto de «Beowulf 2» para indicar importantes modificaciones en lo que hace a la instalacisn, administracisn y distribucisn de procesos en un cluster Beowulf [8, 9]. Esas modificaciones parten de reconocer algunos defectos de los cluster Beowulf originales: adicionar nuevos clientes implica instalar el sistema operativo en ellos y modificar los archivos necesarios en el servidor y en los viejos clientes para que los nuevos sean reconocidos; una actualizacisn de kernel importante hace necesaria la instalacisn de los parches y la recompilacisn de aquel en todos los nodos del cluster; etc.

La aparicisn de los paquetes Scyld [10] y OSCAR [11] tiene la intencis n de facilitar no sslo la instalacisn y administracisn del cluster, sino también las tareas de adicionar nuevos clientes y actualizar versiones de kernel. A modo de ejemplo describiremos con algún detalle la instalacisn de un cluster Beowulf utilizando el paquete Scyld.

Instalando un cluster «Beowulf 2» con Scyld

La versisn básica, sin soporte ni documentacisn, del paquete Scyld puede ser descargada desde ftp://ftp.scyld.com/pub. La última versis n disponible en ese sitio es la 27Bz-7. La notacis n «Bz» es utilizada para indicar que se trata de la versis n básica y diferenciarla así de la versisn comercial, con soporte y documentacis n incluida, identificada como «Cz».

Como se coments anteriormente, es recomendable que la configuracis n del cluster sea como la que se muestra en la figura ya que la instalacisn permite ajustar los parámetros de dos tarjetas de red.



¿Qué es «High Performance Computing»?

El término «High Performance Computing» (computacisn de alto rendimiento) tiene su origen en el trabajo desarrollado por Seymour Cray al diseñar y construir las computadoras que llevan su nombre. Esos sistemas vectoriales proporcionaban un poder de csmputo un orden de magnitud mayor que otros sistemas contemporáneos, razsn por la cual fueron denominadas «supercomputadoras».

El rápido incremento mostrado en nuestros días tanto por la velocidad de los procesadores de computadoras personales como por la relacisn rendimiento/precio que las mismas suministran, sumado al desarrollo de tecnolo-gías de redes de alta velocidad, conducen necesariamente a una profunda transformacis n del concepto original de High Performance Computing. Actualmente, pensar en un sistema para efectuar computacisn de alto rendimiento es pensar en un cluster de computadoras personales utilizando el sistema operativo Linu y efectuando sus tareas bajo un entorno de programacisn en paralelo.

Muchas son las disciplinas que requieren llevar a cabo diariamente computacisn de alto rendimiento como una parte importante de sus actividades. La astronomía, la biología, la física, muchas ramas de la ingeniería, y la química son algunas de esas disciplinas. El procesamiento de imágenes, la determinacisn de la secuencia de los nuclestidos en el ADN y la simulacisn numérica de procesos de interés biolsgico, químico o físico son algunas de las actividades que requieren de la computacisn de alto rendimiento para alcanzar resultados en tiempos razonables.

Podemos decir entonces que la «computa-cis n de alto rendimiento» es aquella dedicada a la resolucisn de problemas bien determinados por medio de sistemas de altísimo poder de csmputo.

No es necesario que el servidor tenga una distribucisn de Linu preinstalada ya que Scyld trae la versisn 6.2 de RedHat.

Una vez establecido en el BIOS el inicio desde la lectora de cd, lo primero que se observa es una instalacisn típica de RedHat. Es altamente recomendable elegir el modo gráfico de instalacisn y luego una instalacisn completa con soporte gráfico en el escritorio Gnome, ya que algunas herramientas del paquete están sslo disponibles en ese modo. Si se tiene suficiente e periencia en instalacisn de Linu , se puede elegir el modo «custom» ya que entonces se evita la instalacisn de muchas aplicaciones que casi seguramente nunca se usarán. En este caso, es conveniente permitir la instalacisn del modo gráfico con el escritorio Gnome por las razones arriba mencionadas.

Sslo una diferencia se puede apreciar respecto a una instalacisn típica de RedHat: una servidor acepta los requerimientos y las direcciones físicas de aquellos aparecen en la ventana derecha de la aplicacisn BeoSetup, «Unknown Addresses». Dichas direcciones se arrastran con el ratsn a la ventana central de BeoSetup, «Configured Nodes», y automáticamente el servidor envía una orden de reinicio a cada diente. El cambio de estado de los dientes resulta evidente al ver la palabra «up» en la columna «Node Status» de la ventana central de BeoSetup. Al mismo tiempo, BeoStatus refleja los cambios producidos al dar de alta los clientes en el cluster.

Los discos duros de los clientes se particionan con la utilidad beofdisk que debe ser invocada desde una consola

```
#>beofdisk -d
#>beofdisk -w
```

Beowulf 2 ha introducido importantes modificaciones en la instalacisn y distribucisn de procesos en un cluster Beowulf.

ventana dedicada a configurar la interfaz eth1, la segunda tarjeta de red. Si se escoge, por ejemplo, una direccisn privada 192.168.1.1 para el servidor, entonces el rango de direcciones a usar debe comenzar en 192.168.1.2 y terminar en 192.168.1.99, siendo 99 un número tentativo (y optimista!), por supuesto.

Una vez finalizada la instalacisn del sistema operativo, el servidor se reinicia y luego de cargar el escritorio automáticamente se inician tres ventanas: una guía de instalacisn rápida de los clientes, la aplicacisn BeoSetup para instalarlos y la aplicacisn BeoStatus para monitorear el estado del cluster.

Los clientes deben poder iniciarse desde el cd de Scyld o desde un disquete que haya sido generado con la utilidad BeoBoot. Ya que resulta engorroso estar llevando el cd de un cliente a otro, es conveniente generar un disquete por cada cliente del cluster. Un botsn para tal fin se encuentra en la ventana de BeoSetup del servidor. Una vez generados los disquetes, se usan para iniciar los clientes.

Lo que sigue es muy interesante: cada diente envía al servidor un requerimiento de direccisn RARP (Reverse Address Resolution Protocol). El

La opcisn -d usa la configuracisn predeterminada para particionar los discos de todos los clientes y -w ocasiona la escritura de la tabla de particisn en los mismos. Para que estos cambios surtan efecto, deben activarse las líneas con informacisn de los sistemas de archivos /dev/hda2 y /dev/hda3 en el archivo /etc/beowulf/fstab y comentar la línea que comienza con $RAMDISK.

Si se desea transferir la imagen de inicio de BeoBoot al disco duro de los dientes, debe ejecutarse

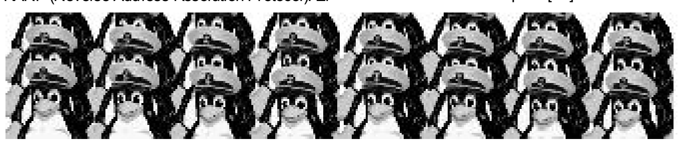
```
#>beoboot-install -a /dev/hda
```

El último paso implica reiniciar todos los clientes, lo cual se efectúa por medio de un único comando desde el servidor

```
#>bpctl -S all -s reboot
```

De esta forma, se tiene un cluster Beowulf instalado y operativo en menos de una hora.

Como broche de oro, el paquete Scyld permite comprobar el rendimiento del cluster por medio de la utilidad Linpack [12].



Lista de referencias

[1] William W. Hargrove, Forrest M. Hoffman, Thomas Sterling, The Do-It-Yourself Supercomputer, edicisn digital de Scientific American (www.scientificamerican.com), agosto 2001.

[2] http://www.top500.org

[3] http://www.oracle.com/ip/deploy/ias/Linu

[4] http://www.epm.ornl.gov/pvm/

[5] http://www.mcs.anl.gov/mpi/inde .html

[6] http://www.lam-mpi.org

[7] http://www-uni .mcs.anl.gov/mpi/mpich

[8] http://www.linu journal.com/article.php?sid=5559

[9] http://www.linu journal.com/article.php?sid=6019

[10] http://www.scyld.com

[11] http://oscar.sourceforge.net, http://www.linu journal.com/print.php?sid=5559

[12] http://www.netlib.org/benchmark/hpl/

*Por **Dr. Reinaldo Pis Diez***

¿Necesito un cluster Beowulf para mis actividades?

No todas las actividades precisan de un alto poder de csmputo para su realizacisn. Por ejemplo, construir un cluster de 4 procesadores para utilizar el procesador de te tos favorito es verdaderamente un desperdicio. Sin embargo el manejo de grandes bases de datos, el tratamiento de imágenes satelitales o la resolucisn de problemas numéricos en diversos campos de la ciencia justifica plenamente la construccisn o adquisicisn de tal cluster o de uno más poderoso.

Básicamente uno podría preguntarse:

*¿Tengo limitaciones de velocidad, memoria, etc. para llevar a cabo mis tareas?

*¿Tengo programas o paquetes de programas que permiten ser ejecutados en paralelo utilizando el paradigma de «message passing»?

*¿Los programas que desarrolla mi grupo pueden ser adaptados para ser ejecutados en paralelo bajo el paradigma anterior?

Si las respuestas a estas preguntas son positivas, entonces debería plantearse seriamente la posibilidad de asesorarse y, eventualmente, construir o adquirir un cluster Beowulf.

Si bien es cierto que todas las ventajas de un cluster Beowulf pueden ser obtenidas por sistemas comercializados por empresas reconocidas internacionalmente, es mundialmente aceptado que un sistema Beowulf proporciona el mismo rendimiento a un costo por lo menos diez veces menor al del sistema comercial.

LPI se asocia con UnitedLinu y Sage



UNITEDLINUX

SAGE

El Linu Professional Institute (LPI) esta entre dos iniciativas que pueden conducir a las diferentes certificaciones Linu a estar mas integradas.

Primero, UnitedLinu , una coalicisn de compañías (incluye a IBM y HP y que ofrece un sistema operativo Linu de base Standard apuntado al usuario de negocios), anuncis en Linu World en NY que el LPI esta ayudando a desarrollar un programa de certificacisn para sus usuarios.

Dos títulos UnitedLinu serán emitidos. UnitedLinu Certified Professional (ULCP) y UnitedLinu Certified E pert (ULCE). Ambos estarán basados en aprobar dos e ámenes LPI mas un único e amen del United Linu program.

Nuestro convenio muestra a la comunidad open souce trabajando juntos para alcanzar un é ito colectivo, comento el presidente de LPI, Evan Leibovitch.

LPI también anuncio que esta investigando una asociacisn con Systems Administrators Guild (SAGE), una divisisn de USENIX que también ofrece un programa de Certificacisn vendedor-neutral.

La asociacisn podría resultar en un arreglo de socios mutuos entre las dos organizaciones, dijeron las compañías. LPI esta ejecutando un buen servicio a la comunidad de administradores de sistemas, y esperamos trabajar sobre los detalles de la asociacisn que culminaran en un arreglo especial de los socios SAGE para aquellos certificados por LPI , dijo el Director Ejecutivo de SAE, Rob Kolstad. SAGE es independiente de vendedor (marcas), tecnologías particulares o filosofías, por eso nuestras organizaciones son compatibles y una buena combinacisn

En el anuncio ninguno comento acerca de csmo la asociacisn podría afectar los programas de certificacisn de las organizaciones.

Para mas informacisn vea: www.lpi.org , www.unitedlinu .com, y www.sage.org

VPN y Linux:
Bajando costos con FreeS/WAN

Hace unos años pensar en utilizar un sistema de VPN sobre Internet para conectar dos sucursales de nuestra empresa parecía una tarea muy compleja, requería conocimientos difíciles de adquirir, y tenía un costo muy alto. Pensar en una VPN sobre una red insegura como lo es Internet era algo descabellado, que brindaba muy pocos beneficios y que, solo era aplicado cuando teníamos que conectar redes remotas en las cuales el proveedor de comunicaciones no nos podía brindar una solucisn la cual se aplicase al presupuesto de comunicaciones. Los tiempos han cambiado, y hoy, se pueden obtener appliances desde 300 U$S que pueden conectar (por lo menos así dice el manual) hasta 16 subredes remotas sobre cualquier enlace WAN o Internet, aparecis el soporte para IPsec en entornos Microsoft junto con L2TP, aparecieron routers CISCO y 3COM y otras tantas compañías que brindan, casi siempre sobre el estándar IPsec, variantes para conectar puntos remotos sobre una red insegura, a un costo relativamente bajo. Ahora llego el turno del software libre que hoy poseen una herramienta poderosísima para manejar VPNs de una manera sencilla y con un alto grado de seguridad. Esta herramienta es llamada FreeS/WAN, Free Secure over WAN. Esta maravilla del software libre es un derivado de un producto llamado S/Wan Secure WAN que con el tiempo fue reemplazado por FreeS/WAN. La idea fundamental de FreeS/WAN es brindar soporte para el protocolo IPsec para el kernel de Linu y mantener un estándar del mismo que permita realizar cone iones hacia otras implementaciones. La misma permite manejar con el estándar IPsec tantos puntos VPN aguante nuestro hardware, es decir, la limitacisn ya no es problema de la administracisn de las redes, sino el hardware en sí mismo, y aun así, logra cumplir su cometido con creces a la hora de establecer VPN con un alto nivel de encriptacisn en los datos y cone iones de gran ancho de banda. Cabe destacar que es posible utilizar FreeS/WAN con hardware dedicado para encriptacisn utilizando alguna de las tantas placas que proveen de chips dedicados a la encriptacisn.

FreeS/WAN conóta de 3 parteó fundamentaleó:

KLIPS: es el soporte del protocolo IPsec dentro de nuestro kernel Linu . Implementa AH, ESP, y manejo de paquetes dentro del kernel. El protocolo AH (Autentication Header) provee autenticacisn de paquetes a nivel kernel. El protocolo ESP (Encapsulating Security Payload) provee encriptacisn más autenticacisn.

PLUTO: demonio IKE, se encarga de negociar las cone iones con otros sistemas. El protocolo IKE (Internet Key E change) es el encargado de negociar los parámetros de una cone isn entre las dos partes participantes.

Diferenteó ócriptó: que automatizan la tarea de administracisn de nuestro Gateway FreeS/Wan agregando rutas cuando sea necesario.

Los modos más tradicionales de uso de FreeS/WAN no tienen nada que envidiarle a otras implementaciones de VPN sobre IPSEC.

Tipoó de Cone ioneó:

Punto a Red: un host que soporta IPsec se conecta a una red entera. Puede acceder a cualquier punto de la misma de manera segura y confiable.

Red a Red: una red entera accede a otra conectándose con IPsec. Se puede acceder en cualquier maquina de ambas redes de manera segura y confiable.

Road-Warrior: son los llamados guerreros del camino . Esta denominacisn es generalmente aplicada a host que se conectan a una red segura pero que tienen ip variable y el tipo de cone isn es indiferente para FreeS/WAN, el único requisito es que este conectado a la misma red insegura , en este caso, Internet, y una notebook que acceda a la misma a través de Dial-Up, ADSL, Cable-Msdem, etc.

FreeS/WAN propone implementar VPNs sobre el estándar IPsec, conectividad con otros productos comerciales, y, una alternativa en los costos de licenciamiento, como todo software libre.

FreeS/WAN puede ser obtenido desde la pagina oficial www.freeswan.org. Cuando hablamos de soporte para IPsec sobre el kernel de Linu estamos hablando de que hay que aplicarle parches a nuestro Linu . Los contribuidores de FreeS/WAN han hecho un e celente trabajo y brindan rpms para las últimas versiones de kernel de RedHat que facilitan ampliamente la tarea del administrador.

Loó rpmó conótan de doó parteó:

Freeówan-module: es el rpm que contiene los msdulos necesarios para dar soporte IPsec sobre nuestro kernel actual.

Freeówan-1.99: son las llamados userland utilities , utilidades a nivel usuario que manejan todo el sistema de ruteo cuando una cone isn es establecida, y el demonio que corre en user-space .

Oportuniótic Encription:

Uno de los puntos fuertes y diferenciadores de FreeS/WAN sobre otras implementaciones es el llamado OE (Oportunistic Encription). El mismo permite que dos gateways FreeS/WAN se comuniquen entre sí encriptando él tráfico, incluso si los administradores nunca han tenido contacto previo y ninguno de los sistemas tenga predefinido informacisn del otro.

Para esto ambos sistemas deben tomar la informacisn de autenticacisn que necesiten de DNS, así, los administradores, solo ingresan su informacisn en el sistema DNS y setean su gateway con OE. Para esto debemos contar con algún servidor DNS que soporte DNSSEC.

Eóta técnica brinda doó grandeó beneficioó:

Reduce el esfuerzo administrativo enormemente para IPsec. Un administrador configura el gateway FreeS/WAN, y todo lo demás es automático, la necesidad de configurar de manera túnel desaparece.

Permite crear un ambiente en el cual la privacidad es un defecto. Todo él trafico será encriptado siempre que el otro lado lo permita.

OE no es todavía un estándar dentro del protocolo IPsec, pero, actualmente se encuentra en proceso de demostracisn para la futura incorporacisn dentro de IPsec. Solo un producto comercial implementa una forma de OE, Secure Sendmail, el cual, automáticamente encripta transferencias de email entre servidores siempre que sea posible.

Cuadro de compatibilidad:

Aquí se define un cuadro de compatibilidad entre FreeS/WAN y otras implementaciones IPsec:

	FreeS/WAN VPN				Road Warrior	OE
	PSK	RSA Secret	X.509 (requiere parche)	Manual Keying		
isakmpd (OpenBSD)	SI		SI	SI		NO
Kame (FreeBSD, NetBSD)	SI		SI	SI		NO
McAfee VPN was PGPNet	SI	SI	SI		SI	NO
Microsoft Windows 2000/XP	SI		SI		Con FreeS/WAN como Warrior	NO
Safenet SoftPK/SoftRemote	SI		SI		SI	NO
SSH Sentinel	SI		SI		SI	NO
otros						
Ashley Laurent VPCom	SI					NO
Borderware	SI				NO	NO
Checkpoint FW-1	SI					NO
Checkpoint VPN1	SI/parcial					NO
Cisco with 3DES	SI					NO
F-Secure	SI					NO
Gauntlet GVPN	SI					NO
IBM AS/400	SI					NO
Lucent	SI					NO
Netscreen 5 p	SI					NO
Nortel Conitivity	parcial					NO
RadGuard	SI					NO
Raptor (NT)	SI			SI		NO
Raptor (Solaris)	SI					NO
Redcreek Ravlin	SI/parcial					NO
Shiva LANRover	SI					NO
Sun Solaris				SI		NO
SonicWall	SI					NO
Timestep	SI					NO
Watchguard Firebo	SI			SI		NO
Xedia Access Point /QVPN	SI					NO

Performance de FreeS/WAN:

Contemplando que se utilice solo software, el encargado de realizar toda la encriptacisn y desencriptacisn de datos, será el procesador, obviamente, afectan factores como el tipo de bus, memoria, etc.

Las siguientes pruebas fueron realizadas:
Gateway A: Pentium Celeron 400 Mhz. 128 MB RAM PC-100. Realtek 8139-c PCI.
Gateway B: Pentium Celeron 400 Mhz. 128 MB RAM PC-100. Realtek 8139-c PCI.

Realizando una cone isn con la compañía Fibertel en un cablemsdem de 128kbps de upstream y 512kbps de downstream la velocidad final de nuestra VPN fue de 128kbps tanto de upstream como de downstream, esto es debido a una limitacisn de nuestro servicio de Internet, y aun así, ambos Linu continuaban con procesador libre como para seguir realizando otras tareas.

Gateway A: Pentium Celeron 400 Mhz. 128 MB RAM PC-100. Modem 56k US ROBOTICS.
Gateway B: Pentium Celeron 400 Mhz. 128 MB RAM PC-100. Modem 56k US ROBOTICS.

En este caso la cone isn se realizo con un proveedor gratuito de Internet, Keko . La velocidad final de la VPN fue de 33.6/33.6 kbps y nuevamente esto se debis a una limitacisn de la cone isn a Internet. El único dato diferencial en esta prueba fue que aunque la velocidad de cone isn es relativamente baja la latencia de la cone isn crecis notablemente.

De Gateway A a Gateway B utilizando como interfaz ppp0 con un ping llegamos a tener latencias entre 180 y 250ms. Mientras que si realizábamos la misma operacisn desde la interfaz ipsec0 (la interfaz virtual de FreeS/WAN) la latencia se incremente entre 230 y 320ms.

Concluóión

FreeS/WAN propone implementar VPNs sobre el estándar IPsec, conectividad con otros productos comerciales, y, una alternativa en los costos de licenciamiento, como todo software libre. La administracisn del mismo es relativamente sencilla y la documentacisn técnica encontrada en el sitio oficial es bastante buena, permitiendo realizar cone iones inmediatamente. La performance es bastante buena pero esta directamente relacionada con la potencia de nuestro hardware. Cabe aclarar que FreeS/WAN puede funcionar en sistemas SMP pero la divisisn de las tareas no llega a un aumento del 35% en la performance.



por ***Ariel Mella***
(MCSE, LPIC-Nivel 2)

OPEN LDAP

El props sito de este artículo es mostrar Open LDAP como el servicio principal de directorios para entornos heterogéneos. El server LDAP permite compartir, por ejemplo, la libreta de direcciones que usamos en nuestro cliente de correo, también provee un login unificado para los usuarios Linu y Windows, automount de directorios home, y comparticisn de archivos para clientes Linu y Windows.

Este artículo está basado en una nota aparecida en el magazine Linu Journal (ampliada en muchas partes) y trata sobre la implementacisn de OpenLDAP, que se llevs a cabo en Midwest Tool & Die, una compañía americana,ubicada en Indiana que se dedica al estampado para la industria automotriz y para la industria electrsnica. La idea surgis hace tres años cuando la compañía necesits compartir la informacisn de sus directorios, y en la impementa-cisn particips el área de ingeniería de la Universidad de Purdue.

Midwest Tool & Die están usando OpenLDAP hace 3 años y su performance ha sido intachable. La compañía vio el primer gran beneficio al compartir los contactos de la agenda electrsnica. Ahora han unificado su logon desde cualquier computadora de la red. Sus usuarios pueden acceder al mismo archivo a través de Windows/Samba o de Linu /NFS/automount.

El articulo lo dividiremos en 2 partes. Una sera la publicada en NEX a modo de introduccion y el articulo completo estara en nuestra web page (www.ne web.com.ar) como archivo pdf de modo de que se pueda hacer un download.

Todo el articulo esta basado en un ejemplo de un entorno simple.

(Vea la Figura 1).

La configuracisn utilizada en este artículo no documenta el uso de SSL. El programa ldap-sync.pl que usa puede e poner su LDAP manager password. Como resultado, los clientes Windows pueden cachear sus passwords de usuario, creando por lo tanto, un nuevo riesgo para la seguridad Linu . (Ni Midwest Tool & Die, ni sus empleados, ni los autores de este artículo, se hacen responsables por su seguridad)

Antes de entrar en la instalacisn y configuracisn del servidor LDAP, veamos un poco más en profundidad de qué se trata.....

Introduccisn

1 ¿Qué es LDAP?

LDAP (Lightweight Directory Access Protocol", «Protocolo Ligero de Acceso a Directorios») es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio.

1.2 ¿Qué es un servicio de directorio?

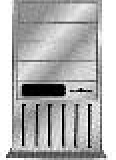
Un directorio es como una base de datos, pero en general contiene informacisn más descriptiva y más basada en atributos. La informacisn contenida en un directorio normalmente es lee mucho más de lo que se escribe. Como consecuencia los directorios no implementan normalmente los complicados esquemas para transacciones o esquemas de reduccisn (rollback) que las bases de datos utilizan para llevar a cabo actualizaciones complejas de grandes volúmenes de datos. Por contra, las actualizaciones en un directorio son usualmente cambios sencillos de «todo o nada», si es que se permiten en algo.

Los directorios están afinados para proporcionar una repuesta rápida a operaciones de búsqueda o consulta. Pueden tener la capacidad de replicar informacisn de forma amplia, con el fin de aumentar la disponibilidad y la fiabilidad, y a la vez reducir el tiempo de respuesta. Cuando se duplica (o se replica) la informacisn del directorio, pueden aceptarse inconsistencias temporales entre la informacisn que hay en las réplicas, siempre que finalmente e ista una sincronizacisn.

E isten muchas maneras distintas de proporcionar un servicio de directorio. Los diferentes métodos permiten almacenar en el directorio diferentes tipos de informacisn, establecer requisitos diferentes para hacer referencias a la informacisn, consultarla y actualizarla, la forma en que protege al directorio de accesos no autorizados, etc. Algunos servicios de directorio son locales, proporcionando servicios a un conte to restringido (por ejemplo, el servicio de finger en una única máquina). Otros servicios son globales, proporcionando servicio en un conte to mucho más amplio.

Figura 1

ldapserver.foo.com

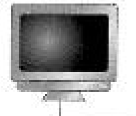


* OpenLDAP Server
* Samba PDC for FCC
* Hosts Users on/home

bigdisk.foo.com

* OpenLDAP Client
* Samba Server
* NFS Server
*Automounts /h, /share

Linu Workstation



* OpenLDAP Client
* Automounts /h, /share
* Mozilla E-mail Client

MS Windows Workstation

* SMB Domain Member of FOO
* Browses Samba Shares
* Mozilla or MS Outlook E press E-Mail Client



1.3 ¿Csmo funciona LDAP?

El servicio de directorio LDAP se basa en un modelo cliente-servidor. Uno o más servidores LDAP contienen los datos que conforman el árbol del directorio LDAP o base de datos troncal. El cliente ldap se conecta con el servidor LDAP y le hace una consulta. El servidor contesta con la respuesta correspondiente, o bien con una indicacisn de dsnde puede el cliente hallar más informacisn (normalmente otro servidor LDAP). No importa con qué servidor LDAP se conecte el cliente: siempre observará la misma vista del directorio; el nombre que se le presenta a un servidor LDAP hace referencia a la misma entrada a la que haría referencia en otro servidor LDAP. Es ésta una característica importante de un servicio de directorios universal como LDAP.

El demonio o programa servidor para el directorio LDAP se llama *slapd* y puede ejecutarse sobre muchas plataformas UNIX diferentes.

Hay otro demonio o programa servidor que se encarga de la replicacisn entre servidores. Su nombre es slurpd y por el momento no necesitará preocuparse de él. En este documento, ejecutaremos un *slapd* que proporciona servicio de directorio para su dominio local únicamente, es decir, sin *slurpd*.

Instalacisn y configuracisn del servidor LDAP

Elegimos bajar los paquetes binarios RPM , instalamos openldap-2.0.11-8 on Red Hat 7.1. También necesita los paquetes auth_ldap y nss_ldap. Usaremos como nombre de dominio foo.com.

Si quiere instalar la última versisn de este paquete, siga las instrucciones para bajarlo e instalarlo de www.openldap.org/doc/admin/quickstart.html

Edite el archivo de configuracisn del server LDAP, que es /etc/openldap/slapd.conf, como sigue:

```
# Schemas to use
    include/etc/openldap/schema/core.schema
    include/etc/openldap/schema/cosine.schema
    include/etc/openldap/schema/inetorgperson.schema
    include/etc/openldap/schema/nis.schema
    include /etc/openldap/schema/redhat/rfc822-MailMember.schema
    include/etc/openldap/schema/redhat/autofs.schema
    include/etc/openldap/schema/redhat/kerberosobject.schema
database    ldbm
 suffi       dc=foo,dc=com
 rootdn      cn=Manager,dc=foo,dc=com
 rootpw     {crypt}sadtrCr0CILzv2
 directory   /var/lib/ldap

inde        default              eq
 inde       objectClass,uid,uidNumber,gid
            Number               eq
inde        cn,mail,surname,givenname
                                 eq,sub

#Acces Control (See openldap v.2.0 Admin Guide)
acces to attr=userPassword
by self                          write
by anonymous                     auth
by dn= cn=manager,dc=foo,dc=com
                                 write
by *    compare
acces to *
 by self                         write
 by dn= cn=manager,dc=foo,dc=com write
 by *                            read
```

LDAP (Lightweight Directory Access Protocol", «Protocolo Ligero de Acceso a Directorios») es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio.

Los schemas LDAP definen clases y atributos de los objetos que componen las entradas al directorio.

Los schemas que necesitamos, listados en la primera seccisn de slapd.conf, ya han sido definidos durante la instalacisn RPM.

Si necesita agregar una clase o un atributo a un objeto, vea la Guía de Administracisn de OpenLDAP en www.openldap.org/doc/admin20/schema.html.

Vamos a usar el tipo de base de datos ldbm, que es el que viene por default, y nuestro ejemplo usa el componente de dominio LDAP. Entonces, foo.com se transforma en dc=foo,dc=com. Además el administrador tiene permiso de escritura sobre todas las entradas LDAP.

La Guía de Referencia de Red Hat 7.3 sugiere usar **crypt** para proteger las contraseñas.

```
perl -e print crypt(´passwd´, ´salt_string´,);
```

Reemplace *salt_string* por un salto de 2 caracteres, y *passwd* por la password en te to plano. El resultado, que es la contraseña encriptada péguela en slapd.conf.

Las líneas inde mejoran la performance para atributos que se consultan con frecuencia.

Acces control restringe el acceso a la entrada de userPassword, pero el usuario y el administrador pueden modificar la entrada. Para todas las demás entradas, el administrador tiene permiso de escritura y los demás usuarios, de lectura.

por **Ing. Alejandra García**

Usted pude encontrar el artículo completo en www.ne web.com.ar donde se desarrollan los siguientes puntos:

*Creando la Estructura de Directorios
*Compartir contactos de Libreta de Direcciones
*Configuracisn de Clientes de Correo
*Unificando el logueo Linu con LDAP
*Creando entradas de usuario en la Máquina Local
*Creando Entradas de Grupos
*Configure Automount para compartir Directorios Home (y comparticisn por NFS)
*Configurando el cliente Linu LDAP
*Configuracisn final del servidor Linu
*Login unificado de Microsoft Windows con Samba y LDAP
*Configuracisn de ldapsync.pl y Samba
*Compartiendo recursos NFS con Samba
*Mantenimiento

MS FRONTPAGE VS MACROEMDIA DREAMWEAVER





Al comparar un software con el otro debemos tener en cuenta que ambos en su contracara generan codigo HTML y JavaScript entre otros lenguajes y que por lo tanto la diferencia entre ambos es su inerface visual y su canal operativo por lo que la usabilidad de los mismos depende del usuario y sus preferencias.

El MS Frontapge es muy bueno como programa para principiantes con poco o ningún conocimiento de HTML, ademas permite utilzar modelos o preformatos de diseño de pagina para construir su Web site en minutos. Dar fromato al te to e insertar imágenes de forma tan fácil como usar cualquier otro procesador de te tos, con el cual la mayoría de la gente es familiar.

En consecuencia podriamos decir que el FP está más orientado hacia el consumidor en general.

El Macromedia Dreamweaver es un programa en el cual es necesario tener un conocimiento básico o una nocisn de HTML y JavaScript. Tambien es importante conocer la forma de organizar y distribuir los archivos para poder crear un optimo mapa del sitio. Debemos señalar que su asimilacisn pueda resultar mas compleja en relacisn al MS Frontpage pero la capacidad del programa y sus resultados marcan diferencias y mas aún en su nueva versisn MX que fusionan al Dreamweaver 4 y al Dreamweaver Ultradev permitiendo utilizar las ultimas tecnologias con un potente editor de csdigo.

Como resultado podriamos definir que el DW está orientado hacia los diseñadores de Web con un perfil mas profesional.

Microsoft SQL Server 2000

Al empezar a escribir esta nota no se me ocurría como titularla: SQL 2000vs. SQL 7, Mejoras en SQL 2000, Porque Migrar a SQL 2000, etc., y como verán opte por el mas fácil quizás para no desmerecer la versisn anterior que ha tenido muy buena aceptacisn en el mercado y de paso facilitarme el dilema.

La gente de Redmond (MSFT) ya hace un tiempo, puso en el mercado la actualizacisn de su producto SQL 7.0, el cual este ultimo fue un cambio significativo respecto de su antecesor 6.5 en cuanto al csdigo principal del programa (fue reescrito), pero veremos que su versisn 2000 no se queda atrás en cuanto a aditamentos y mejoras se trata.

Vamos con algunas de las mejoras/cambios principales incorporadas en esta versisn:

Soporte XML:

Para aquellos que no escucharon de XML, eXtensible Markup Language vendría a ser una e tensisn del ya conocido HTML pero orientado a manejar datos, imaginen esto: pedir paginas vía http (como HTML) pero que en la solicitud de esas formatos sin requerir del servidor Web y por otro lado, XML, al ser estándar, es soportado por todo los navegadores (browsers) actuales.

Múltiples Instancias:

Esto nos da la posibilidad de poder tener varias instancias (instances) de MSSQL SERVER 2000 corriendo (hasta 16) y que para cada una, haya un juego aparte de entradas del registro, configuracisn, procesos, etc. en un mismo servidor, lo que seria como instalar varias veces MSSQL SERVER 2000 en una misma maquina.

Ahora se puede tener un servidor por cada DB o cada tantas DB, lo cual permitiría varias cosas, entre estas:

Bajar un servidor/instancia SQL SERVER sin afectar otros servidores/instancias SQL SERVER para tareas de mantenimiento por ejemplo

Poseer distinta configuracisn de servidor (DB Master) o diferentes requisitos de seguridad para cada servidor/instancia.

Poseer un juego de caracteres y sort order (collation) predeterminado distinto para cada servidor/instancia, aunque en esta versisn, a

La gente de Redmond (MSFT) ya hace un tiempo, puso en el mercado la actualizacisn de su producto SQL 7.0, el cual este ultimo fue un cambio significativo respecto de su antecesor 6.5 en cuanto al csdigo principal del programa (fue reescrito), pero veremos que su versisn 2000 no se queda atrás en cuanto a aditamentos y mejoras se trata.

paginas vayan consultas (queries), gracias a las cuales el Server http vinculado a SQL SERVER nos devuelve resultados en otras paginas. ¿Suena a ASP no? pero bueno esto no se parecen en nada ya que difiere significativamente en varios aspectos y poseen diferentes fines, de hecho ASP al igual que otros similares (PHP, etc.) seguirán e istiendo.

Pero veamos algo de lo que se puede hacer con XML:

*Acceder, manipular y actualizar documentos XML como si se tratara de tablas usando lenguaje Transact SQL

*Hacer consultas en la URL usando lenguaje SQL

*Controlar la forma en la cual devuelve los resultados (shapes)

*Etc.

MS SQL 2000 puede generar XML en diferentes diferencia de la anterior, ya se soporta todo esto personalizado por cada DB.

Todo esto lo hace propicio para bajos presupuestos de hardware o consolidacisn de hosteo como el de los ISP's

Versiones:

MS SQL SERVER 2000 fue sacado al mercado con versiones tan potentes como la Enterprise para entornos Data Center, así como en versiones compactas para entornos portátiles como la versisn de las handelds con Windows CE

Escalabilidad:

En cuanto a la escalabilidad en cluster para balance carga cabe mencionar el soporte mediante un sistema de vistas particionadas que resulta en transacciones y consultas distribuidas en múltiples servidores.

Respecto a la escalabilidad en un solo maquina, el soporte de sistemas de hasta 64 GB de RAM y/o 32 procesadores

Performance:

Tiempos de consulta más rápidos gracias a las mejoras en el optimizador de consultas, soporte de vistas inde adas, índices en columnas con campos calculados y soporte completo de multiprocesamiento simétrico (SMP) con lectura de tablas en paralelo.

Ej.; Algunos clientes e perimentaron mejoras de hasta un 300% en sus aplicaciones.

Confiabilidad:

Cluster a prueba de fallos simplificado de hasta 4 nodos, mejora en los tiempos de hacer backup diferenciales, Stand-by Servers mejorado gracias a la característica Log Shipping

incorporada, creacisn y recreacisn de índices en paralelo (más rápido restore) así como la certificacisn de seguridad C2 otorgada por la Nacional Security Agency (NSA) le confieren a MSSQL SERVER 2000 mejoras en este aspecto.

DataWarehouse:

MSSQL SERVER 2000 incorpora un nuevo motor para el datamining.

La habilidad de vincular cubos, que le dan un aspecto multidimensional a los datos, sobre Internet, así como particionar los mismos en diferentes servidores que a su vez le confieren mayor escalabilidad.

Rollups customizados, soporte de nuevos tipos de dimensiones, Ej. parent-child y dimensiones modificables (write-enabled)

OLAP Actions que es una característica que permite disparar eventos en una DB.

Productividad del Programador Mejorada:

Aparte de la adicisn del e tenso entorno XML, MSSQL SERVER 2000 provee a los desarrolladores de la actualizacisn en cascada con integridad referencial para las acciones Update y Delete incorporada, un depurador T-SQL, Triggers del tipo INSTEAD OFF y AFTER y mejoras en el Query Analyzer que incluye plantillas (templates) para la creacisn de scripts administrativos

Como se puede apreciar las mejoras no son pocas y por ende los motivos para migrar o conocer estas nuevas características tampoco.

Microsoft ha puesto en el mercado por medio de las Certified Technical Education Centers (CTEC) una serie de cursos que nos permiten especializarnos en este producto. Dichos cursos sirven también para certificar e ámenes que cuentan para la obtencisn de las certificaciones MCDBA, MCSE y MCSD. Aquí se detallan los más importantes

+Course 2071: Querying Microsoft SQL Server 2000 with Transact-SQL (16 horas)

+Course 2072: Administering a Microsoft SQL Server 2000 Database (40 horas)

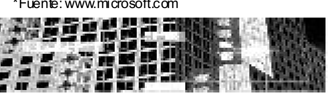
+Course 2073: Programming a Microsoft SQL Server 2000 Database (40 horas)

+Course 2074: Designing and Implementing OLAP Solutions Using Microsoft SQL Server 2000 (40 horas)

La carrera Microsoft Certified Database Administrator MCDBA que consta de 4 e ámenes se puede ver detallada en este link: http://www.microsoft.com/traincert/mcp/mcdba/requirements.asp

por ***Germán Döuek***
MCT/MCSE

*Fuente: www.microsoft.com



Preguntas Microsoft para Examen 70-210

El Área de Psicología del Hospital Cognitive Inc. usa un Domain Controller (Server1) para guardar sus trabajos en una Carpeta compartida en la red de Windows 2000 llamada DOC.

Dora, una Psicsloga con el rango de Administradora de la red por sus vastos conocimientos en Computacisn, cres una subcarpeta llamada SrK en la carpeta compartida DOC. Mediante el Windows E plorer en Computer3, ella navega en la carpeta SrK y se da cuenta de que uno de sus archivos, CasoSigmund.doc fue borrado.

Dora restaura este archivo desde una copia hecha el día anterior y configura los permisos NTFS para que sslo ella pueda acceder al mismo.

Debido a que los archivos restantes de su carpeta deben quedar disponibles para toda el Área de Psicología, Dora ingresa en los permisos NTFS de los mismos y los configura de forma tal que sslo tenga acceso a ellos el grupo de Psicología (lo hace removiendo todos los grupos menos Psicología desde la opcisn seguridad en las propiedades de los archivos), luego le da a este grupo el permiso Read.

Ahora ella quiere saber si alguien que no pertenece al grupo de Psicología procura ingresar en esa carpeta o si alguien intenta borrar nuevamente al CasoSigmund.doc.

E amine el cuadro que muestra la distribucisn de las Áreas del Hospital:

¿Qué debería hacer Dora para determinar quien intenta acceder a sus archivos? (Seleccione todas las correctas)

A) Ella debería configurar a las Group Policy para activar la auditoria en Computer3

B) Ella debería configurar a las Group Policy para activar la auditoria en la Carpeta DOC

C) Ella debería configurar a las Group Policy para activar la auditoria en Server1

D) Ella debería auditar todas las entradas e itosas a la carpeta DOC

E) Ella debería auditar todas las entradas e itosas a la carpeta SrK

F) Ella debería auditar todos los intentos fallidos de entrada a la carpeta DOC

G) Ella debería auditar todos los intentos fallidos de entrada a la carpeta SrK

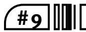
Rta: C,E,G

Las 10 Certificaciones mas buscadas para 2003

El presente estudio fue elaborado por certcities.com (http://certcities.com/editorial/features/story.asp?EditorialsID=55). El estudio se bass en crecimiento, reputacisn y aceptacisn de la industria. A esto se le agregaron otros factores: utilidad, puede hacer una diferencia en la carrera?, Cuál brillara mas?. Aunque el estudio fue hecho en US creemos es de mucho interés para el mercado local.

#10 Empate

Citri Certified Enterprise Administrator (CCEA), Microsoft Certified Database Administrator (MCDBA)
Vendor: Citri , Microsoft
Category: **Networking, Database**
Reader Interest Score (out of 20): **9, 12**
Buzz Score (out of 10): **6, 3**
Total: **15, 15**



#9

Sun Certified System Administrator for Solaris Operating Environment
Vendor: Sun Microsystems
Category: **Linu /Uni**
Reader Interest Score (out of 20): **13**
Buzz Score (out of 10): **3**
Total: **16**



#8

Microsoft Certified Systems Administrator (MCSA)
Vendor: Microsoft
Category: **Windows Networking**
Reader Interest Score (out of 20): **10**
Buzz Score (out of 10): **7**
Total: **17**

#7

Linu +
Vendor: Computing Technology Industry Association (CompTIA)
Category: **Linu /Uni**
Reader Interest Score (out of 20): **16**
Buzz Score (out of 10): **2**
Total: **18**

#6

Check Point Certified Security Administrator (CCSA)
Vendor: Check Point
Category: **Security**
Reader Interest Score (out of 20): **11**
Buzz Score (out of 10): **8**
Total: **19**

#5

Certified Information Systems Security Professional (CISSP)
Vendor: International Information Systems Security Certification Consortium (ISC2)
Category: **Security**
Reader Interest Score (out of 20): **14**
Buzz Score (out of 10): **7**
Total: **21**

#4

Cisco Certified Network Professional (CCNP)
endor: Cisco Systems
Category: **Security**
Reader Interest Score (out of 20): **16**
Buzz Score (out of 10): **6**
Total: **22**

#3

Red Hat Certified Engineer (RHCE)
Vendor: Red Hat
Category: **Linu /Uni**
Reader Interest Score (out of 20): **16**
Buzz Score (out of 10): **7**
Total: **23**

#2

Security+
Vendor: CompTIA
Category: **Security**
Reader Interest Score (out of 20): **18**
Buzz Score (out of 10): **7**
Total: **25**

#1

Cisco Certified Internetwork E pert (CCIE)
Vendor: Cisco Systems
Category: **Networking**
Reader Interest Score (out of 20): **18**
Buzz Score (out of 10): **9**
Total: **27**

Las que estuvieron muy cerca...
1-Oracle Certified Database Administrator (OCP DBA)
2-Microsoft Certified Associate Developer (MCAD)
3-Linu Professional Institute, Level I
4-Sun Certified Web Component Developer
5-SANS GIAC

Certificaciones MCP

MCP	871.433
MCSE	196.533
MCSD	42.004
MCDBA	106279
MCSA	58.297
MCAD	2.746
MCT	10.732

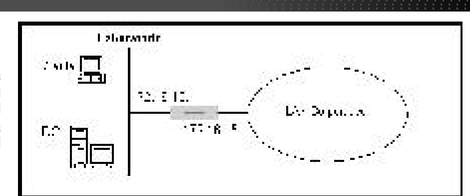
Nº de Certificaciones 1.288.024
Datos Marzo de 2003

Preguntas Microsoft

Pregunta 70-218

Usted esta configurando un laboratorio para testear un ambiente de Windows 2000. Usted instala una PC cliente y un servidor, luego usted promueve el servidor a Domain Controller para el único dominio que e iste en su red corporativa. La configuracisn de red es presentada en el siguiente cuadro de la derecha: Cuando usted intenta unir a la PC cliente al dominio, se recibe un mensaje de que no se encuentra el dominio. Usted revisa la configuracisn TCP/IP en la PC cliente y muestra la siguiente configuracisn:





Usted debe corregir el problema que le impide a la PC cliente unirse al dominio.
¿Cuál de las siguientes opciones debería realizar usted:

A- Especifique el default gateway con el IP 172.16.15.1
B- Especifique el default gateway con el IP 172.16.10.1
C-Cambie la direccisn IP del servidor DNS por la direccisn IP del Domain Controller
D- Especifique la direccisn del DC como DNS alternativo
Rta: B

70-214 Nuevo e amen de Seguridad Microsoft

Desde Comienzos del 2003 está operativo un nuevo e amen de Microsoft que apunta a la seguridad en redes:
70-214 Implementando y Administrando Seguridad en una red Microsoft de Windows 2000 .
Éste e amen puede incluirse como elective en la currícula de MCSA (Microsoft Certified System Administrator) y MCSE (MS Systems Engineer).
Para ver más detalles de los e puestos en éste artículo:
www.microsoft.com/traincert/e ams/70-214.asp

EVENTOS

CONFERENCIAS TÉCNICAS MICROSOFT 2003
ACTUALIqATE. FUTURIqATE.

Nuevas técnicas en el desarrollo de aplicaciones Web con ASP.NET. Tips & Tricks

MSDN Conferencia Tecnica 22 de Mayo de 2003, ASP.NET, 10:00 a 13:00 hs
Bouchard 710, 4 Piso, Capital Federal
Descripcisn: Migrando a ASP.NET - Tips y Trucos en ASP.NET,
Orador: Daniel Laco, MVP - Carlos Walzer, MVP, Nivel: Intermedio,
Audiencia: Desarrollador

MSDN Conferencia Tecnica 19 de Junio de 2003, Threads en .NET + Elementos de Remoting en .NET, 10:00 a 13:00 hs, Bouchard 710, 4 Piso, Capital Federal, Descripcion: Threads en .NET. Csmo desarrollar aplicaciones distribuidas con .NET Remoting, Orador: Angel Lspez, MVP - Julio Novomisky, MVP, Nivel: Intermedio, Audiencia: Desarrollador

MSDN Conferencia Tecnica 26 de Junio de 2003, Conceptos de Arquitectura para el diseño de Aplicaciones distribuidas, 10:00 hs a 13:00 hs
Bouchard 710, 4 Piso, Capital Federal
Descripcion: Consideraciones de diseño/arquitectura de aplicaciones para desarrolladores o responsables de equipos de desarrollo
Orador: Adrian Lasso, MVP
Audiencia: desarrollador, arquitectos de aplicaciones, responsable de equipos de desarrollo

Por favor regístrese en: http://www.microsoft.com/argentina/conferencias_tecnicas. Todos estos eventos son gratuitos, las vacantes son limitadas. Para registrarse visite nuestros sites de: TechNet MSDN O por e-mail a eventos@microsoft.com.ar